学校编码：**10384** 分类号 _____ 密级 _____

学　　号：**19020090153598** **UDC**_____

厦门大学

博 士 学 位 论 文

几个公钥密码方案和几个变换半群

Several Public Key Cryptography Schemes
And Several Semigroups Of Transformations

邓 伦 治

指导教师姓名：曾 吉 文 教授
专 业 名 称：基 础 数 学

论文提交日期：2012 年 4 月
论文答辩日期：2012 年 6 月
学位授予日期：2012 年 月

答辩委员会主席：_____
评　　阅　　人：_____

2012 **年　月**

厦门大学学位论文原创性声明

兹呈交的学位论文，是本人在导师指导下独立完成的研究成果．本人在论文写作中参考的其它个人或集体的研究成果，均在文中以明确方式标明．本人依法享有和承担由此论文而产生的权利和责任．

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人完全了解厦门大学有关保留、使用学位论文的规定. 厦门大学有权保留并向国家主管部门或其指定机构送交论文的纸质版和电子版，有权将学位论文用于非赢利目的的少量复制并允许论文进入学校图书馆被查阅，有权将学位论文的内容编入有关数据库进行检索，有权将学位论文的标题和摘要汇编出版. 保密的学位论文在解密后适用本规定.

本学位论文属于

1、保密（　　），在　　年解密后适用本授权书.

2、不保密（　　）.

（请在以上相应括号内打”✓”）

作者签名:　　日期:　　年　月　日

导师签名:　　日期:　　年　月　日

摘 要

本文包括两方面的内容，一是提出了几个新的公钥密码方案；二是研究了几个变换半群的结构。

• 公钥密码 (Public Key Cryptography，简记为 PKC) 是实现网络和信息安全的重要技术。传统的公钥设施 (Public Key Infrastructure，简记为 PKI) 要求设立一个可信中心，由其向个人发放证书，将个人的身份与公钥邦定，这就要求进行证书管理。为解决上述问题，1984 年，Shamir 提出了一种新的公钥体制：基于身份的密码方案，其要求建立一个可信第三方 — 私钥生成中心 (Private Key Generator，简记为 PKG)，由其根据每个成员的身份，向每个成员提供私钥，这又导致了密钥托管的问题。 2003 年， Al-Riyami 和 Paterson 提出了无证书公钥密码体制，其可以看成是传统公钥体制和基于身份公钥体制的结合。其要求设立一个半可信的第三方 — 私钥生成中心 (Key Generate Center，简记为 KGC)，每个成员的私钥由两部分组成，一是自己设定的私钥，二是由 KGC 根据成员个人的身份发放给成员的部分私钥，这样既解决了密钥托管的问题，也不需要证书。本文提出了几个基于身份和无证书的密码方案。

• 由于任何一个抽象半群都能嵌入到一个变换半群中，就从理论而言，对于半群理论的研究，只要研究变换半群就足够了。一直以来，由于有限变换半群优良的可计算性和一系列的组合性质使其受到广大半群学者的青睐。 1951 年， J.A.Green 首次研究了格林关系，格林关系在半群理论的发展中扮演着基础性作用的角色，特别是在有限变换半群理论的发展中。给定一个拓扑空间 X，则 X 上的所有连续自映射在映射合成运算下构成一个半群。设 E 是集合 X 上的一个等价关系，则 X 构成一个拓扑空间，其中由所有的 E 类集合构成 X 拓扑的拓扑基。本文对几个保等价关系的变换半群进行了研究。

关键词: 基于身份密码，无证书密码，加密，签名，签密，半群，变换，等价关系，序

Abstract

This paper includes two parts: several new public key cryptography schemes are proposed and several semigroups of transformations are studied.

• Public key cryptography is an important technique to realize network and information security. Traditional public key infrastructure requires a trusted certification authority to issue a certificate binding the identity and the public key of an entity. Hence, the problem of certificate management arises. To solve the problem, in 1984, Shamir defined a new public key paradigm called identity-based public key cryptography which needs a trusted private key generator (PKG) to generate a private key for an entity according to his identity. So we are confronted with the key escrow problem. In 2003, Al-Riyami and Paterson introduced the notion of certificateless public key cryptography, which can be conceived as an intermediate between traditional public key infrastructure and identity-based cryptography. It lets a semi-trusted key gerenate center (KGC). The person's secret key includes two parts: a self-generated user secret key and user partial key which is issued by KGC with respect to every one own identity. In this paper, several identity-based and certificateless cryptography schemes are proposed.

• Since each semigroup can be inseted in some transformation semigroup. Theoretically, for abstract semigroup theory it is enough to study transformation semigroup. Finite full transformation semigroup has attacted many scholars thanks for it is computable and it has many well combinatorial properties. Green′s relations, first studied by J.A.Green in 1951, have played a fundamental role in the development of semigroup, especially, in the development of finite full transformation semigroup. All continues selfmaps of a given topological spaces X make up of a semigroup under composition. Let E is an equivalence on a set X, then X be endowed with the topology for which the family of all E-classes is a basis. In this paper, several semigroups of transformations that preserve an equivalence are studied.

Keywords: Identity-base cryptography; Certificateless cryptography; Encryption; Signature; Signcryption; Semigroup; Transformation; Equivalence; Order.

目 录

Contents

第一部分： 几个公钥密码方案

第一章：研究背景与基础知识

§1.1 公钥密码简介

公钥密码 (PKC) 是实现网络和信息安全的重要技术手段。传统的公钥设施 (PKI) 要求设立一个可信中心，由其向个人发放证书，将个人的身份与公钥邦定。因此，证书管理的问题出现了，为解决上述问题， 1984 年， Shamir 提出了一种新的公钥密码体制：基于身份的密码方案 [1] ，其要求建立一个可信第三方 – 私钥生成中心 (PKG) ，由其根据每个成员的身份，向每个成员提供私钥，这又导致了密钥托管问题的出现。幸运的是，刚才提到的两个问题都能被无证书公钥密码体制解决 [2] ，其可以看成是传统公钥密码体制和基于身份公钥密码体制的结合。

公钥密码体制的概念是由 Diffie 和 Hellman 于 1976 年提出的，也被称为非对称密码体制，公钥密码体制是密码学历史上最突出的发展。在当时，所有的经典的密码系统都是对称的密码体制，也就是通信双方共享一个秘密密钥，此密钥既能用于加密也能用于解密，这就导致了一些密钥分配问题。例如：对于一个密码系统，我们必须通过安全信道将秘密密钥分配给通信用户，如果有 N 个成员的话，则有 C_n^2 个秘密密钥必须交换，也就需要 C_n^2 条安全信道，而且每个用户必须储存 $N-1$ 个密钥，即使对一个相当小的网络，也可能变得相当昂贵。如果一个秘密密钥泄露了，则攻击者能够用此秘密密钥解密所有用此秘密密钥加密的消息 (至少两个用户被攻破) 。此外，对称密码体制难以实现认证，无法提供不可否认性服务。因此，对称密码体制难以满足开放性环境的需求。

公钥密码体制通过将密钥分成两部分而解决了上述密钥分配问题，即分成公开密钥 (公钥) 和私有密钥 (私钥) 。公开密钥被记录在一个公共的数据库中，私有密钥被用户秘密地保存。这样，公开密钥能被用于加密消息，而在解密过程中用户必须知道私有密钥。公钥密码学所提供的另一个重要贡献是数字签名，数字签名能够提供认证服务和不可否认服务，对保证电子商务过程中的各种交易的安全可靠性具有重要意义。

公钥密码体制的设计比对称密码体制的设计具有更大的挑战性，因为公钥为攻击算法提供了一定的信息，事实上公钥密码体制无法提供无条件安全，所以我们仅研究公钥密码体制的计算安全性，目前所使用的公钥密码方案的安全性基础主要是数学中的难解问题，正是公钥密码体制思想的提出，使数学逐渐在密码学中扮演重要角色 (对称密码体制的基础学科主要是物理学和计算机科学) 。公

钥密码体制的加密速度虽然不如对称密码体制快，尤其在加密数据量较大时，但它易实现认证。因此，实际工程中常采用的解决办法是将公钥密码体制和对称密码体制结合，即公钥密码体制用来分配密钥，对称密码体制用于加密消息。

基于身份的加密 (Identity-Based Encryption，简记为 IBE) 是一种公钥密码体制，其公钥可以是个人的身份证号码，电子邮箱号码，或者驾驶执照号码等等。在基于身份的加密体制中，有一个被认为是高度可信任的第三方 — 私钥生成中心 (PKG)，它利用自己所掌握的主密钥 (Master Secret Key) 向需要私钥的个人发放私钥。为了对一个消息进行加密，加密者只需知道接收者的身份，当接收到密文后，接收者利用他自己的私钥就可解密密文。

Shamir 基于 RSA 密码体制，给出了一个基于身份的签名方案 [1]。1988 年，Guillou and Quisquater 利用零知识辨别协议，构造了一个类似于 RSA 基于身份签名方案 [3]。2001 年，Boneh 和 Franklin 设计了一个高效的基于身份的公钥加密方案 [4]，在他们的方案中，使用了双线性对这一工具，这是一种可以在某些椭圆双曲线上构造出来的映射。伴随着这一工具的出现，大量的基于身份的加密，签名，密钥管理等方案被相继提出，所有这些密码方案都利用了双线性对这一工具。然而，找到合适的椭圆双曲线，进而构造出高效的双线性对不是一件容易的事，因此，构造高效的，没有利用双线性对的密码方案依然是有现实意义的。

2001 年，Shamir 和 Tauman[5] 基于单向陷门函数正式提出了环签名的概念。在一个环签名方案中，真实签名者选择其他几个成员，加上他自己构成一个环，不需要其他成员的帮助，就能代表整个环对消息进行签名，并且能让任何的检验者确定消息是被环中某位成员所签，但又不能确定到底哪一位成员是真实签名者。自从环签名概念提出后，相继又提出了具有各种功能的环签名，例如：门限环签名 [6]，基于身份的环签名 [7]，签名者能自证的环签名 [8]，代理环签名 [9]。第一个标准模型下高效的环签名方案 [10] 由 Shacham 和 Waters 给出。

第一个基于身份的环签名方案出现在文献 [11] 中。此后，文献 [12,13,14] 给出了几个更加高效的构造，文献 [15] 指出并修正了文献 [11,12] 中一些错误。文献 [16] 给出了一个基于身份的环签名方案和一个基于身份的来自匿名子集的环签名方案 (方案中是由 n 个群组成的环，而不是由 n 个人组成的环)。J.Herranzit[17] 基于难解的 RSA 问题，给出了一个新的基于身份的签名方案，此方案没有利用双线性对。文献 [18,19] 给出了具有固定签名长度的基于身份的环签名方案。

近年，出现了一些具有特定性质的门限环签名方案。Liu 等人在门限环签名中引入了可分离性这一概念 [20]，使得在同一个门限环签名中，能使用各种不同的公钥。Tsang 等人把个体关联性引入到门限环签名方案中 [21]，使任何人能确定两个门限环签名是否是由同一个人所签。Chan 等人构造了盲门限环签名方

案 [22] 。文献 [23] 给出了第一个基于身份的门限环签名方案，此后，文献 [24,25] 给出了另两个基于身份的门限环签名方案，文献 [26,27] 给出了没有利用双线性对的基于身份的门限环签名方案。

1997 年， Yuliang Zheng 提出了一种新的密码体制 – 签密 [28] ，其能同时实现数字签名和公钥加密这两种功能，并且比传统的先签名再加密的做法具有更低的计算成本。文献 [29-34] 给出了几个具体的签密方案。文献 [35] 给出了签密的一个正式的安全证明。在门限环签密方案中，任意 t 个使用者，任意选择另外 $n-t$ 个人，再加上他们自己，构成含有 n 个成员的环，然后使用他们自己的私钥和环中所有成员的公钥对消息进行签密，这一过程并不需要另外那 $n-t$ 个人的同意和帮助，并且最终的密文并不会泄露到底哪些是真正的签密者。门限环签密对于要求至少 t 个人合作，以匿名，可认证，机密的方式泄露一个可靠的秘密是非常有用的。

2005 年， XinYi Huang 把环签名的思想引入到基于身份的签密体制当中，给出了基于身份的环签密方案 [36] 。 2008 年， Fagen Li 等人给出了一个高效的基于身份的环签密方案 [37] ，同年， Lijun Zhun 等人给出了一个高效的基于身份的签名方案和签密方案 [38] 。 2009 年， ZhenChao Zhu 等人给出了一个高效的可以证明安全的基于身份的环签密方案 [39] 。然而， Sree Vivek S 等人指出了文献 [37] 中的方案是不安全的 [41] ， S. Sharmila Deva Selvi 等人指出文献 [38,39] 中的方案是不安全的 [42] 。

2005 年， Sahai 和 Waters[42] 提出了基于属性加密的思想 (Attribute-Based Encryption ，简记为 ABE) ，其实质是一种新的访问控制结构。在基于属性加密体制中，有一个可信任的第三方，由其向使用者发放私钥。使用者的私钥和被加密的密文是与一组属性相关联的。一个使用者，如果他的私钥和密文之间符合某种匹配，其才能解密密文。属性加密概念提出后，学者们提出了许多改进和扩张方案 [43-48] 。 2006 年， Goyal 等人在 Sahai 和 Waters 的属性加密的基础上，将特征集合交集较大的解密条件扩展成一般的单调访问结构，构造出可支持细粒度访问控制的密钥规则下的方案 [45] ，引入一般秘密分享的思想，其访问结构为一般单调访问结构，大大扩展了基于属性加密的应用范围。该方案的提出，丰富了基于属性加密的性质和适用范围，大大加速了基于属性加密相关研究的发展。 2007 年， Bethencourt ， Sahai 和 Waters 给出密文规则下基于特征的加密方案 [44] ，将访问结构与密文相关联，为密文指定能解密的用户。后来， Chase[47] 提出多中心的基于属性加密方案，从而降低了对每个属性中心的信任度，即每个属性中心只掌管一部分属性。

近年来，一些学者试图构造基于属性的签名方案 (Attribute-Based Signature ，

简记为 ABS)，与其类似的一个概念 – 模糊身份签名在文献 [49,50] 中被提出，其允许具有属性 ω 的签名者，利用其中一部分属性对消息签名，而检验者能检查消息是否是被某个具有这样属性的用户所签。基于属性签名在文献 [51] 中被正式提出，随后，一些方案被相继提出 [52,53] 。

组合基于属性加密和基于属性签名概念，对处理复合的认证和访问控制问题提供了一种很好的方法，例如，一个公司的人事部经理，想向公司内的某个部门秘密的发送一个文件，要求，只有指定部门的员工能解密文件，且其能确认这一文件发自人事部的某个成员，那这时，基于属性的签密 (Attribute-Basd Signcryption，简记为 ABSC) 就能解决这一问题。文献 [54] 中给出了一个基于属性的门限签密方案。

2003 年， Al-Riyami 和 Paterson 提出了无证书公钥密码体制的概念 (Certificateless Public Key Cryptography，简记为 CL-PKC)，其目的就是消除基于身份密码体制中的密钥托管问题，随后，很多安全高效的方案被相继提出 [55-64] 。在无证书密码方案中，不仅没有密钥托管，也没有证书管理。它要求建立一个半可信的第三方 – 私钥生成中心 (Key Generate Center，简记为 KGC)，由其根据用户的身份，生成用户的部分私钥，并通过安全通道发送给用户。用户的私钥由两部分组成：私钥生成中心发送的部分私钥和自己选取的密钥，用户的公钥由用户根据自己选取的密钥而设定。在无证书密码体制中，其安全性，要考虑两种不同类型敌手的攻击：第一种，称为公钥代换攻击，敌手能够代换用户的密钥 / 公钥对，但是，对于其向攻击的目标用户，敌手无法获取目标用户的部分私钥。第二种，称为恶意的但被动的私钥生成中心攻击，即私钥生成中心就是恶意的敌手，其拥有系统主密钥，因此任何用户的部分私钥他都能自己生成，但是，对于其想攻击的目标用户，其不能代换此目标用户的密钥 / 公钥对。

在过去的几年中，对无证书签名做了很多的研究，但对于无证书环签名的研究相对比较少 [65-69]，只有两个无证书门限环签名方案 [68,69] 。 Chow 和 Yap 给出了一个无证书环签名方案 [65] 和安全模型，但其安全性不是最强的，且没有考虑恶意但被动的私钥生成中心敌手攻击，在计算效率方面，其总共需要进行 n 次双线性对的计算，因此，当 n 比较大时，其计算成本很昂贵。 Zhang 等人给出另一个无证书环签名方案 [66] 和更强一些的安全模型，但其依然没有考虑恶意但被动的私钥生成中心敌手攻击，在计算效率方面，其总共所需进行的双线性对计算的次数是一个常数，比方案 [65] 具有一定的优势，但其签名算法，需要进行 n 次方幂运算。 H.Q.wang 等人提出了分布式无证书环签名的概念，并给出了一个具体的方案 [67]，其要求计算的双线性对的次数与真实签名者的人数成线性关系。 S.Chang 等人正式提出了无证书 (t, n) 门限环签名方案的安全模型，并给

出了一个具体的无证书环签名方案和 (t,n) 门限版本 [68] 。 H.Q.Wang 等人给出了一个能证明安全的无证书门限环签名方案 [69] ，其总共需要 $6n-2t$ 双线性对的计算。

§1.2 预备知识

双线性映射. 设 G_1 和 G_2 是两个阶为素数 q 的循环群， g 是群 G_1 的一个生成元。 $e: G_1 \times G_1 \to G_2$ 是满足下列条件的一个映射：

1. 双线性性：对于任意的 $g_1, g_2 \in G_1$ 和 $a, b \in_R Z_p$ ，有 $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$ 。

2. 非退化性：存在 $g_1, g_2 \in G_1$ 使 $e(g_1, g_2) \neq 1$. 也就是说， e 并不把 $G_1 \times G_1$ 中的所有元素都映射成 G_2 中的单位元。

3. 可计算性：对于任意的 $g_1, g_2 \in G_1$ ，存在一个高效的算法计算 $e(g_1, g_2)$.

定义 1.1 给定 G_1 和 G_2 是两个阶为素数 q 的循环群， g 是群 G_1 的一个生成元。 $e: G_1 \times G_1 \to G_2$ 是双线性映射，已知 (g^a, g^b, g^c) 和 $X \in G_2$, 判定双线性 Diffie-Hellman 问题 (DBDHP) 是：问等式 $X = e(g,g)^{abc}$ 是否成立。

定义 1.2 给定 g 是素数 q 阶循环群 G_1 的一个生成元，已知 (g^a, g^b) 和 $X \in G_1$, 判定 Diffie-Hellman 问题 (DDHP) 是：问等式 $X = g^{ab}$ 是否成立。

定义 1.3 给定 g 是素数 q 阶循环群 G_1 的一个生成元，已知 (g^a, g^b), 计算 Diffie-Hellman 问题 (CDHP) 是：计算 g^{ab} 。

定义 1.4 给定 g 是素数 q 阶循环群 G_1 的一个生成元，和 $g^a \in G_1$, 离散对数问题 (DLP) 是：计算 a 。

定义 1.5 给定 p, q 是两个 k 比特的素数， $N = pq$ 。 l 是一固定参数， b 是一个随机选择的素数， $b > 2^l$ 且 $\gcd(b, \varphi(N)) = 1$ 。 Y 是从 Z_N^* 中随机选出来的一个数， RSA 问题是：找到 $X \in Z_N^*$ 使 $X^b = Y \bmod \mathrm{N}$ 。

第二章：基于身份的门限环签名方案

§2.1 基于身份的门限环签名方案的模型

基于身份的门限环签名方案包括四个算法：系统初始化算法，密钥生成算法，签名算法和验证算法。

系统初始化：输入安全参数 k，私钥生成中心 (PKG) 生成系统的公共参数。

密钥生成：输入用户的身份 $ID \in \{0,1\}^*$， PKG 计算相应的私钥 S_{ID}，并通过一个安全通道把 S_{ID} 传送给用户 ID 。

签名；输入 n 个用户身份构成的集合 $W = \{ID_1, ID_2, \cdots, ID_n\}$，其中 $t \leq n$ 个用户的私钥 $\{S_{ID_{i_j}}\}(1 \leq i_j \leq n)$ 和消息 m 。输出一个基于身份的 (t,n) 门限环签名 σ 。

验证：输入 (t,n) 门限环签名 σ, 消息 m, 和用户身份集合 $W = \{ID_1, ID_2, \cdots, ID_n\}$ 。如果 σ 是 W 中至少 t 个用户对消息 m 的签名，则输出 1，否则，输出 0 。

定义 2.1 如果所有多项式时间算法敌手 $\mathcal{A}$ 在下面游戏中的优势 $Adv(\mathcal{A})$ 是可忽略的，则称这个基于身份的门限环签名方案在选择消息和身份攻击模型下是不可伪造的 (EUF-IBTRS-CMIA) 。

系统初始化：挑战者 $\mathcal{A}$ 输入安全参数 k，运行系统初始化算法，将系统参数 $param$ 告诉敌手 $\mathcal{A}$ 。

查询：敌手 $\mathcal{A}$ 执行多项式次数的自适应查询，即每次查询都可以根据前面查询的结果作出。

Hash 函数查询：敌手 $\mathcal{A}$ 可以询问 Hash 函数值。

密钥生成查询：敌手 $\mathcal{A}$ 选择一个用户身份 ID，传送给挑战者 $\mathcal{C}$， $\mathcal{C}$ 调用密钥生成算法计算 S_{ID}，并把结果传送给敌手 $\mathcal{A}$ 。

签名查询：敌手 $\mathcal{A}$ 选择 n 个用户身份构成的集合 $W = \{ID_1, ID_2, \cdots, ID_n\}$, 和任意的消息 m，挑战者 $\mathcal{C}$ 输出一个基于身份的 (t,n) 门限环签名 σ 。

伪造：敌手 $\mathcal{A}$ 输出一个伪造的基于身份的 (t,n) 门限环签名 σ，签名身份集合 $W = \{ID_1, ID_2, \cdots, ID_n\}$, 和被签名的消息 m 。要求： σ 不是通过前面的签名查询而得到， W 中至多有 $t-1$ 个用户的私钥被查询过。如果 σ 能通过验证算法，则称敌手 $\mathcal{A}$ 获胜。

敌手 $\mathcal{A}$ 的优势就定义为其获胜的概率。

定义 2.2. 任意选择 n 个用户身份构成集合 $W = \{ID_1, ID_2, \cdots, ID_n\}$, W 中 $t \leq n$ 个用户的私钥 $\{S_{ID_{i_j}}\}(1 \leq i_j \leq n)$，和任意的消息 m，通过签名算法得到 σ 。如果对于任意的验证者 (此验证者不能为 W 中成员)，即使其有无限的计算能力，