圆锥曲线公钥密码导引

YUANZHUI QUXIAN GONGYAOMIMA DAOYIN

王　标／编著

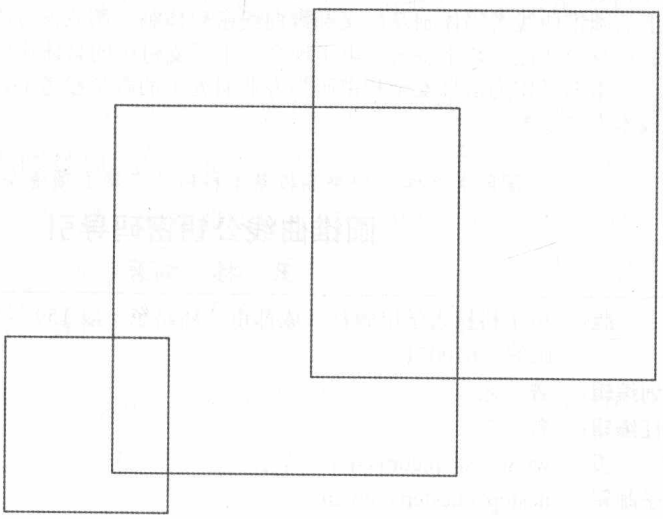
电子科技大学出版社

国际关系学院中央高校基本科研业务费专项资金资助项目

圆锥曲线公钥密码导引

YUANZHUI QUXIAN GONGYAOMIMA DAOYIN

王　标／编著



电子科技大学出版社

图书在版编目（CIP）数据

圆锥曲线公钥密码导引 / 王标编著. -- 成都 : 电子科技大学出版社, 2017.1

ISBN 978-7-5647-3859-4

Ⅰ. ①圆… Ⅱ. ①王… Ⅲ. ①圆锥曲线－公钥密码系统 Ⅳ. ①TN918.2

中国版本图书馆 CIP 数据核字(2016)第 205766 号

内 容 简 介

圆锥曲线是一门古老而内容丰富的数学分支。自 1996 年提出基于圆锥曲线的整数因子分解算法后，圆锥曲线在密码学和计算数论中得到了进一步发展。随着以椭圆曲线密码为代表的代数曲线密码体制的快速应用，圆锥曲线密码也引起了更多研究人员的关注。圆锥曲线密码属于公钥密码，它可以提供与 RSA、ElGamal 等公钥密码体制同样的功能，其安全性建立在圆锥曲线离散对数问题、模数 n 的大数分解问题的困难性之上，计算效率优于椭圆曲线密码。本书分三部分系统研究了圆锥曲线公钥密码，第一部分介绍并进一步研究了有限域上 F_p 上和 F_2^n 上的圆锥曲线密码体制及广义圆锥曲线密码体制；第二部分定义并系统研究了环 Z_n 上、$Z[\omega]$以及 Z_2^1 上的圆锥曲线密码体制及广义圆锥曲线密码体制。第三部分给出了圆锥曲线密码体制在身份认证、数字签名、电子现金、电子支付中的具体应用。

本书可作为信息安全和密码学专业研究生的教学参考书，也可供相关专业工程技术人员参考。

国际关系学院中央高校基本科研业务费专项资金资助项目

圆锥曲线公钥密码导引

王 标 编著

出　　版：电子科技大学出版社（成都市一环路东一段 159 号电子信息产业大厦 邮编：610051）
策划编辑：曾　艺
责任编辑：曾　艺
主　　页：www.uestcp.com.cn
电子邮箱：uestcp@uestcp.com.cn
发　　行：新华书店经销
印　　刷：三河市明华印务有限公司
成品尺寸：170mm×240mm　　印张 10.5　　字数 220 千字
版　　次：2017 年 1 月第一版
印　　次：2017 年 1 月第一次印刷
书　　号：ISBN 978-7-5647-3859-4
定　　价：64.00 元

前　言

1996 年，张明志引进了有限域 F_p 上圆锥曲线 $C_p(a,b)$ 上的加法运算，证明了曲线上的点与引进的运算构成一个有限加群，并提出了用圆锥曲线分解整数的方法，这为构造圆锥曲线密码(Conic Curve Cryptography, CCC)提供了可能。1998 年，曹珍富提出了基于有限域上圆锥曲线的公钥密码体制，随后，又提出了 RSA 的圆锥曲线模拟，这些工作引起了密码研究人员的关注。由于 CCC 中明文嵌入、阶的计算、逆元的计算、点的运算都比较容易，这些对设计公钥密码算法具有很大吸引力。因此，CCC 成为继椭圆曲线公钥密码之后，研究人员比较关注的代数曲线类公钥密码体制。在前人研究基础上，本书系统研究了有限域上、环上的圆锥曲线的性质，研究了有限域上、环上的圆锥曲线、广义圆锥曲线公钥密码体制，包括公钥密码算法和数字签名方案。本书共 7 章，分三个部分。

第一部分介绍并系统研究了有限域上圆锥曲线及其公钥密码体制：一是就有限域 F_p 上圆锥曲线的离散对数问题、明文嵌入的编码和译码算法、ElGamal 算法模拟、基于圆锥曲线点阵列的 Hill 分组加密的实现、安全参数选择等作了进一步研究；二是介绍了有限域 F_{2^n} 上的圆锥曲线公钥密码 $(C_{F_{2^n}}(a,b),\oplus)$，就相关密码性质等作了进一步的研究；三是进一步研究了有限域上广义圆锥曲线 $R_p(a,b,c)$ 的运算性质，给出了 $R_p(a,b,c)$ 的一种分类和阶的计算，进一步研究了 $R_p(a,b,c)$ 的性质。

第二部分定义并系统研究了环 Z_n 上的圆锥曲线 $C_n(a,b)$、广义圆锥曲线 $R_n(a,b,c)$ 及其性质：一是定义了 $C_n(a,b)$，以两种方式对 $C_n(a,b)$ 进行了刻划，一种是直接以坐标的方式给出 $C_n(a,b)$ 中全体有理点的表示，另一种是在 $C_n(a,b)$ 和 $C_p(a,b)\times C_q(a,b)$ 间建立一一对应映射 φ，给出了 $C_n(a,b)$ 的阶；二是在 $C_n(a,b)$ 上定义了两种加法运算：一种是由点的坐标直接定义运算，另一种是通过映射 φ 的逆映射 φ^{-1} 及孙子定理来定义，并证

明了这两种运算是相同的，记为⊕，同时，证明了$C_n(a,b)$对所定义的运算⊕构成一个有限加群，记为$(C_n(a,b),\oplus)$；三是对$(C_n(a,b),\oplus)$的一些基本性质作了较深入的讨论，对$(C_n(a,b),\oplus)$的研究表明，其明文嵌入、阶的计算、点之间的运算、求逆元等运算比椭圆曲线密码体制上的计算要容易，这些性质使得圆锥曲线公钥密码在设计实现中有自身的优势；四是定义了$R_n(a,b,c)$上的Ⅰ类和Ⅱ类曲线，证明Ⅰ类曲线等价于$C_n(a,b)$，可用于构造公钥密码体制，同时指出Ⅱ类曲线不宜用来构造公钥密码体制；五是定义了只涉及移位和按位的模2加法运算的环Z_{2^l}上的圆锥曲线$\mathrm{C}_{Z_{2^l}}(a,b)$，证明了$\mathrm{C}_{Z_{2^l}}(a,b)$上的点在定义的加法运算⊕下构成了一个有限交换群，可用于构造公钥密码体制，并研究了相关密码性质。

第三部分是构造了$C_p(a,b)$、$C_n(a,b)$、$R_n(a,b,c)$、$\mathrm{C}_{Z_{2^l}}(a,b)$等加群上的各类公钥密码算法和数字签名方案，分析了相关密码性质：一是得出$C_n(a,b)$上的RSA公钥密码算法和经典RSA算法一样，安全性建立在大数分解的困难性之上，可以抵抗现有针对小指数的攻击，比经典RSA算法更安全，具有应用前景；二是给出了环Z_n上的椭圆曲线$E_n(a,b)$上的KMOV方案和QV方案在$C_n(a,b)$上的模拟，与经典RSA签名算法相同，新算法的安全性建立在大数分解的困难性基础之上，在抵抗小指数攻击方面比经典RSA算法更安全，$C_n(a,b)$的这两个方案与$E_n(a,b)$上的方案相比，不仅保留了原方案的优点，且计算量要少，也容易实现，特别是$C_n(a,b)$上的QV方案在安全曲线选择较$E_n(a,b)$上有很大提高；三是给出了圆锥曲线密码体制在身份认证、数字签名、电子现金、电子支付中的一些具体应用。

本书的编写和出版得到了国际关系学院中央高校基本科研业务费专项资金资助（项目编号：KYF-2011-T26，KYF-2012-T09），特此感谢。

作　者

目　录

1 导 论

1.1 引 言

随着计算机技术和现代通信技术的成熟、宽带的广泛应用、互联网普及程度的快速提高，社会信息化步伐明显加快，使得基于网络通信和计算机应用技术的电子商务、电子政务等各种网络化的社会活动受到了全世界的广泛关注，并得到了极其迅猛的发展。

然而，尽管我国网上交易和电子政务等每年以相当高的年增长率快速发展，持“犹豫态度”的消费者或使用者都表示，网络的安全性是他们的最大顾虑，他们对网络服务最担心的是被人恶意侵犯隐私，被人偷盗银行账号、密码，被人非法篡改信息等等。事实也证明，网络的风险是普遍性的。据统计，全球约 20 秒钟就有一次计算机入侵事件发生，网络上有 1/4 的防火墙被突破，约 70%的网络信息主管报告因机密信息泄漏而受损，包括病毒、漏洞等引发的安全事件更是数不胜数。

总的来说，网络服务的用户主要的担心是信息的机密性（Confidentiality）、完整性（Integrity）、可用性（Availability）受到破坏，换句话说，用户就是希望系统能够保障数字信息的有效性。为保障信息的机密性、完整性和可用性三性，有许多技术手段，其中广义的公钥密码技术是一种基础性的重要技术手段，包括公钥密码加密技术、数字签名技术等。

本书主要研究一类较新型的密码体制——圆锥曲线公钥密码体制。

1.2 关于圆锥曲线及其密码体制的研究

1.2.1 研究背景

自从 Diffie 与 Hellman[1]提出公钥密码体制以来，各种公钥密码算法

不断涌现。根据公钥密码体制的安全基础来分类，现有的被公认为安全、实用、有效的公钥密码体系有三类。

1．基于大整数因子分解问题的公钥密码体系

这一类公钥密码体系基于大整数因子分解的困难性，其中，最著名的当属 RSA 公钥密码体系。该算法是由麻省理工学院的三位学者于 1977 年提出的[2]，是目前被广泛接受并实现的通用公钥密码体系之一。

2．基于有限乘法群上离散对数问题的 DLP 类公钥密码体系

DLP 类公钥密码体系是基于有限乘法群上的离散对数问题的求解困难性的，其中最著名的有 E1Gamel 公钥密码算法[3]。

3．基于代数曲线有限加法群上的离散对数问题的公钥密码体系

在这一类公钥密码体系中，著名的有椭圆曲线公钥密码体系 ECC，其数学基础是有限域上椭圆曲线有限加法群上的椭圆曲线离散对数问题的求解困难性。它是由华盛顿大学的 Neal Koblitz 和 IBM 公司的 Victor Miller 于 1986 年各自独立地提出的[4]，近 20 年来发展很快。在同等安全条件下，椭圆曲线公钥密码体系具有许多独到的优势，因而成为当前的一个研究热点。

代数曲线密码体制引起人们更多关注，除了椭圆曲线外，是否还存在类似、甚至在某些方面更好的代数曲线，用以构造公钥密码体制。

1996 年张明志引进了圆锥曲线 $C_p(a,b)$ 上的加法运算[5]，并证明曲线上的点与引进的运算能构成一个有限加群，提出了用圆锥曲线分解整数的方法，这也为构造圆锥曲线密码体制提供了可能性。1998 年，曹珍富提出了基于有限域上圆锥曲线的公钥密码体制[6]，随后，他又提出了 RSA 的圆锥曲线模拟[7]，这些工作引起了密码研究人员的关注。2000 年，戴宗铎、裴定一、杨君辉等提出了有限域上的广义圆锥曲线 $R_p(a,b)$，定义了曲线上的加法，并证明 $R_p(a,b)$ 是一个加群以及 $R_p(a,b)$ 中的离散对数问题不比有限域中的离散对数困难[8]。尽管如此，由于 $(C_P(a,b),\oplus)$ 中明文嵌入、阶的计算、逆元的计算、点的运算都比较容易，2002 年，孙琦、张起帆、彭国华指出用整数的标准二进制表示（国外称 NAF），存在一个快速计算 $(C_P(a,b),\oplus)$ 中群元整数倍的算法[9,10]。这些对设计密码算法具有很大吸引力。1992 年 K.Koyama, U.Maurer, T.Okamoto, S.Vanstone 在文

献[11]中，2000 年 Ming hua Qu,Scott vanstone 在文献[12]中分别提出了基于大数 n（$n=pq$）分解困难性的环 Z_n 上的椭圆曲线的数字签名方案（分别简称 KMOV 方案、QV 方案），克服了经典 RSA 算法无法抵抗小指数攻击，QV 方案还克服了前者所具有的同态性的缺点。2003 年和 2005 年，朱文余和孙琦对环 Z_n 上的椭圆曲线的基本性质作了深入的研究，进一步改进了 KMOV 方案和 QV 方案[13,14]。但是，$E_n(a,b)$ 上计算复杂，使我们联想到，如果能把有限域上的圆锥曲线推广到环 Z_n 上，类似 $E_n(a,b)$ 那样建立运算，证明环 Z_n 上的圆锥曲线 $C_n(a,b)$ 和广义圆锥曲线 $R_n(a,b,c)$ 也是一个加群，那么，同样可以建立各种公钥密码协议。它们不仅保留了 $E_n(a,b)$ 中的优点，而且计算更简单，特别对于 RSA 类型的公钥密码算法，在 Z_n 上的圆锥曲线 $C_n(a,b)$ 构成的加群上，变得更安全、更具有应用前景。近年来，本书作者及合作者作了一些研究工作，主要发表在文献[15-23]中。

1.2.2 研究内容和主要贡献

本书系统地研究了环上圆锥曲线的性质，构造环上圆锥曲线的公钥密码体制和数字签名方案，并进一步研究了环上广义圆锥曲线的性质及其公钥密码体制。

主要的创新工作如下：

1．对环 Z_n 上的圆锥曲线 $C_n(a,b)$ 及其性质作了系统的研究

（1）类似有限域 F_p 上的圆锥曲线 $C_p(a,b)$，定义了环 Z_n 上的圆锥曲线 $C_n(a,b)$。

（2）用两种方式对 $C_n(a,b)$ 进行了刻划：一种是直接以坐标的方式给出 $C_n(a,b)$ 中全体有理点的表示，得到 $C_n(a,b)=C_1\cup C_2\cup C_3\cup O$；另一种是在 $C_n(a,b)$ 和 $C_p(a,b)\times C_q(a,b)$ 间建立一一对应映射 φ，十分方便地给出了 $C_n(a,b)$ 的阶。

（3）在 $C_n(a,b)$ 上定义了两种加法运算：一种是由点的坐标直接定义运算，另一种是通过映射 φ 的逆映射 φ^{-1} 及孙子定理来定义，并证明了这

两种运算是相同的，记为⊕。同时，证明了$C_n(a,b)$对所定义的运算⊕构成一个有限加群，记为$(C_n(a,b),\oplus)$。

（4）对$(C_n(a,b),\oplus)$的一些基本性质作了较深入的讨论，包括离散对数问题、阶的计算、基点G的寻求等。指出如何通过$C_p(a,b)$和$C_q(a,b)$的性质来证明$C_n(a,b)$的性质。

通过对$C_n(a,b)$的研究，表明各种公钥密码体制在$C_n(a,b)$上的模拟是可行的。

（5）定义了只涉及移位和按位的模2加法运算的环Z_{2^l}上的圆锥曲线$C_{Z_{2^l}}(a,b)$，证明了$C_{Z_{2^l}}(a,b)$上的点在定义的加法运算⊕下构成了一个有限交换群，并研究了相关密码性质。

2．构造了$C_n(a,b)$上的各类公钥密码体制，对其实现和应用作了较深入的研究分析

（1）对（$C_n(a,b),\oplus$）的研究表明，其明文嵌入、阶的计算、点之间的运算、求逆元等运算比椭圆曲线密码体制上的计算要容易。

（2）给出经典的RSA型和ElGamal型公钥密码算法在（$C_n(a,b),\oplus$）上的模拟以及数值例子。

（3）分析了经典RSA算法所面临的威胁，如小指数攻击。指出$C_n(a,b)$上的RSA公钥密码算法和经典RSA算法一样，其安全性建立在大数分解的困难性之上，但由于可以抵抗现有针对小指数的攻击，其比经典RSA算法更安全，更具有应用前景。

（4）给出了环Z_n上的椭圆曲线$E_n(a,b)$上的KMOV签名方案和QV签名方案在$C_n(a,b)$上的模拟，与经典RSA签名算法相同，新算法的安全性建立在大数分解的困难性基础之上，在抵抗小加密指数和小解密指数攻击方面比经典RSA算法安全。$E_n(a,b)$上的KMOV方案具有同态性，$E_n(a,b)$上的QV方案克服了这一缺点，但是其使用具有很大局限性。基于$C_n(a,b)$的这两个方案与基于$E_n(a,b)$的方案相比，不仅保留了原方案的优点，而且在$C_n(a,b)$上，计算量要少得多，也容易实现，特别是对于

QV 方案的圆锥曲线模拟，在实现上较 $E_n(a,b)$ 上有很大提高，因此，$C_n(a,b)$ 上的这两个签名方案更具应用价值。

（5）总结了电子现金和电子支付系统的研究发展现状，归纳了盲签名和群签名技术的发展以及在电子支付系统中的重要作用，并指出经典 RSA 型盲签名和群签名方案所面临的安全问题。

（6）给出了 RSA 型盲签名方案在 $C_n(a,b)$ 上的模拟及其数值示例。类似的，与经典的 RSA 型盲签名方案相比，建立在 $C_n(a,b)$ 上签名方案的安全性得到一定的提高，特别是在抵抗小加密指数和小解密指数攻击方面比经典 RSA 算法安全，因此，$C_n(a,b)$ 上的盲签名具有应用价值。并将新的签名方案应用到可分电子现金系统中。

（7）给出了 RSA 型群签名方案在 $C_n(a,b)$ 上的模拟及其数值示例。同样，与经典的 RSA 型群签名方案相比，建立在 $C_n(a,b)$ 上签名方案的安全性得到一定的提高，并将该签名方案应用到电子货币发行子系统中。

（8）指出诸如公平盲签名、群定向签名以及多重数字签名等各类签名方案均可以在 $C_n(a,b)$ 上实现模拟，并在安全性上得到进一步的提高。

3．对广义圆锥曲线及其公钥密码体制进行了较系统的研究

（1）对有限域 F_p 上广义圆锥曲线 $R_p(a,b,c)$ 的性质作了研究，并给出 $R_p(a,b,c)$ 的有理点所满足的方程，有理点的坐标表示和阶的计算等。

（2）定义了环 Z_n 上的广义圆锥曲线 $R_n(a,b,c)$。

（3）较系统地研究了 $R_n(a,b,c)$ 的一般性质，以两种方式对 $R_n(a,b,c)$ 进行了刻划：一种是以坐标的方式给出了 $R_n(a,b,c)$ 中全体有理点的表示，得到 $R_n(a,b,c)=R_1\cup R_2\cup R_3\cup O$；另一种方式是在 $R_n(a,b,c)$ 和 $R_p(a,b,c)\times R_q(a,b,c)$ 间建立一一对应映射 φ，十分方便地给出了 $R_n(a,b,c)$ 的阶。

（4）在 $R_n(a,b,c)$ 上定义了两种加法运算：一种是由点的坐标直接定义，另一种是通过映射 φ 的逆映射 φ^{-1} 及孙子定理来定义，并证明这两种运算是相同的，记为 $\oplus$。

（5）指出如何通过 $R_p(a,b,c)$ 和 $R_q(a,b,c)$ 的性质来证明 $R_n(a,b,c)$ 的性质，证明了 $R_n(a,b,c)$ 对于定义的运算 $\oplus$ 构成一个有限加群，记为 $(R_n(a,b,c),\oplus)$。

（6）证明了当假定运算过程在 R_1 中进行时，可用点的参数表示来进行；对 $(R_n(a,b,c),\oplus)$ 的一些基本性质作了深入讨论，包括离散对数问题、阶的计算等，这些为构建 $R_n(a,b,c)$ 上的公钥密码体制提供了可能性。

（7）给出了 $R_p(a,b,c)$ 的一种分类，并将 $R_p(a,b,c)$ 的分类推广到 $R_n(a,b,c)$ 上，研究了它们的离散对数问题，定义了环 Z_n 上的 I 类和 II 类广义圆锥曲线。

（8）证明了 I 类广义圆锥曲线 $R_n(a,b,c)$ 等价于环上的圆锥曲线 $C_n(a,b)$，可用于构造公钥密码体制，同时，指出 II 类广义圆锥曲线 $R_n(a,b,c)$ 不宜用来构造公钥密码体制。

（9）在 I 类 $R_n(a,b,c)$ 上，给出了 RSA 型加密方案和 KMOV 数字签名方案的模拟，并给出 KMOV 数字签名方案的数值模拟实例。

（10）指出一些经典的公钥密码算法和数字签名方案，如 QV 数字签名方案、盲签名方案、群签名方案以及公平盲签名方案等等，均可以在 $R_n(a,b,c)$ 上实现模拟，并在安全性、计算效率和实现方面有一定程度的提高。

1.3 本书内容结构

全书共分为七章。

第一章是绪论，介绍了本书的著作背景，所研究的内容、主要研究成果和全书的整体结构框架。

第二章主要介绍了公钥密码学中常用的代数和数论基础，包括圆锥曲线的标准定义和非标准形式，群、环、域等相关概念，以及常用的数论基础知识。

第三章主要讨论有限域上的圆锥曲线及其公钥密码体系。包括有限

域F_p上的圆锥曲线及其公钥密码体制、有限域F_{2^n}上的圆锥曲线及其公钥密码体制，研究了有限域上圆锥曲线密码体制的一些一般性问题，给出了常见公钥密码算法的具体实现过程，并讨论了有限域上的广义圆锥曲线在公钥密码学应用中的实际问题。

第四章定义并研究了环Z_n上的圆锥曲线及其公钥密码体制。包括定义了环Z_n上的圆锥曲线及其有限加群，讨论了其在公钥密码体制中计算分析等问题，设计了基于环Z_n上圆锥曲线的RSA密码算法、ElGamal密码算法和Rabin数字签名方案，最后研究并讨论了环Z_n上广义圆锥曲线及其公钥密码体制的具体实现问题。

第五章主要研究设计了基于环Z_n上圆锥曲线$C_n(a,b)$上的KMOV和QV签名方案及其具体实现过程，分析了$C_n(a,b)$上KMOV、QV签名方案比环上椭圆曲线$E_n(a,b)$上的相应方案具有更好的密码特性，包括计算量和曲线选择等，并给出了上述方案以参数表示形式的数值模拟。

第六章定义并研究了环Z_{2^l}上的圆锥曲线$C_{Z_{2^l}}(a,b)$及其公钥密码体制，讨论了其安全性，模拟了$C_{Z_{2^l}}(a,b)$上ElGamal加密方案，并指出$C_{Z_{2^l}}(a,b)$上的各项运算适合软件和硬件的设计与实现。

第七章主要研究圆锥曲线公钥密码的各种应用。包括基于有限域F_p上圆锥曲线的零知识身份鉴别方案，对基于环Z_n上的圆锥曲线的xiao06数字签名方案进行了有意义的改进，将基于环Z_n上圆锥曲线的盲签名方案应用在可分电子现金中，将基于环Z_n上圆锥曲线的群签名方案应用在电子支付系统中。

1.4 参 考 文 献

[1] W.Diffie and M.E.Hellman. New directions in cryptography. IEEE Transactions on Information Theory, Vol.22, No.6, pp.644-654（1976）.

[2] Rivest R L, Shamir A and Adleman L. A method for obtaining digital signatures and public key cryptosystems[J]. Comn. ACM, 1978, 21:120-126.

[3] ElGamal, L. A public key cryptosystem and a signature scheme based on the discrete logarithm. IEEE Transactions on Information Theory, 1985, 31（4）: 469-472.

[4] Koblitz, N. Elliptic Curve Cryptosystems. Mathematics of computation, 48（1987）, pp.203-209.

[5] 张明志. 用圆锥曲线分解整数[J]. 四川大学（自然科学版），1996，33（4）：356-359.

[6] 曹珍富. 基于有限域F_p上圆锥曲线的公钥密码系统. 密码学进展—Chinacypt'98，北京：科学出版社，1998，45-49.

[7] 曹珍富. RSA与改进的RSA的圆锥曲线模拟[J]. 黑龙江大学自然科学学报，1999（4）：15-18.

[8] Zong-Duo Dai, Ding-Yi Pei, Jun Hui Yang, Ding-Feng Ye. Cryptanalysis of a Public Key Cryptosystem Based on Conic Curves. The International Workshop on Cryptographic Techniques&E-Commerce（Hong Kong,2000）.

[9] 孙琦，张起帆，彭国华. Dickso多项式$g_e(x,1)$公钥密码体制的新算法[J]. 四川大学学报（自然科学版），2002（1）：18-23.

[10] 孙琦, 张起帆, 彭国华. 计算群元的整数倍的一种算法及其在公钥密码体制中的应用. 密码学进展——ChinaCrypt'2002, 第七届中国密码学学术会议论文集. 北京：电子工业出版社，PP117-124.

[11] K.Koyama, U.Maurer, T.Okamoto, and S.A.Vanstone. New Public-Key Schemes Based on Elliptic Curves over the Ring Z_n. Advances in Cryptology__CRYPTO'91, Lecture Notes in Computer Science No.576, Springer-Verlag, pp.252-266（1992）.

[12] Ming hua Qu, Scott Vanstone. On ID-Based Cryptosystems over Z_n. 庆贺柯召院士九十寿辰暨国际数论学术研讨会上的报告，2000年7月.

[13] 朱文余，孙琦. 环Z_n上椭圆曲线及数字签名方案[J]. 电子与信息学报（原电子科学学刊）2003年增刊，Vol.25,40-47.

[14] 朱文余，孙琦. 环Z_n上椭圆曲线的密钥交换协议[J]. 电子学报，2005（1）：83-87.

[15] 王标，方颖珏，林宏刚等. 基于环Z_n上圆锥曲线的QV签名方