文章编号:1671-9352(2013)05-0001-13 DOI:10.6040/j.issn.1671-9352.9.2013.003

椭圆曲线在密码中的应用:过去,现在,将来…

张方国
(中山大学信息科学与技术学院,广东 广州 510006)

摘要:从19世纪开始,数学家们就把椭圆曲线的算术性质作为代数、几何和数论的一个研究目标进行深入研究。至今,椭圆曲线的理论不仅应用在数学领域,还被广泛应在计算科学、信息安全、物理学等领域。本文主要综述一下椭圆曲线理论在密码学领域的应用,从最早的素性检测、整数分解到椭圆曲线密码体制,以及双线性对密码体制和最近的抗击量子计算的椭圆曲线同种密码体制,对这些应用的基本原理和研究及应用现状逐一介绍。最后对这一领域的一些公开问题和可能的未来进展作了简单探讨。

关键词:椭圆曲线;密码学;离散对数;双线性对;同种
中图分类号:TN911 **文献标志码**:A

Elliptic curves in cryptography: past, present and future…

ZHANG Fang-guo
(School of Information Science and Technology, Sun Yat-sen University, Guangzhou 510006, Guangdong, China)

Abstract: From the beginning of the nineteenth century, mathematicians have put the elliptic curves as a research objective of algebra, geometry and number theory to study in-depth. So far, the theory of elliptic curves applied not only in the field of mathematics, and also widely in computing science, information security, physics and other fields. In this paper, we reviewed the application of elliptic curves in cryptography, from the primality testing, integer factorization to elliptic curve cryptosystem, bilinear pairing based cryptosystem and the quantum-resistant cryptosystems from elliptic curve isogenies. We introduced the basic principles and the status of these applications. Finally, we briefly discussed some open questions and possible future progress in this area.

Key words: elliptic curve; cryptography; discrete logarithm problem (DLP); bilinear pairing; isogenies

0 引言

椭圆曲线是一个域上的三次不定方程所定义的一种平面曲线,在数学理论研究中最初是属于几何研究范畴,但该曲线与微积分(主要是椭圆积分:一种包含三次或四次多项式的平方根的积分,来自椭圆周长的计算)有密切联系,所以椭圆曲线渗透到微分几何和微分函数理论中。数论中的同余数问题(Congruent Number Problem)可以归结到某种特殊形式的椭圆曲线是否存在非平凡有理数解的问题,从而椭圆曲线又成了数论及代数数论中的一个重要研究内容。在椭圆曲线上可以引入代数运算(群运算),可以利用代数这个工具来研究椭圆曲线这个几何对象,因此椭圆曲线自然又属于了代数几何的研究范畴。1994年Wiles教授利用椭圆曲线理论证明了著名的费马大定理,使得椭圆曲线在数学领域的地位更加突出。关于椭圆曲线理论的著作有很多,根据所要研究的内容或解决的问题,每本书描述的侧重点有所不同。Joseph Sliverman的*The*

收稿日期:2013-03-07; **网络出版时间**:2013-04-23 16:06
网络出版地址:http://www.cnki.net/kcms/detail/37.1389.N.20130423.1606.002.html
基金项目:国家自然科学基金资助项目(61070168,U1135001);高等学校博士学科点专项科研基金资助项目
作者简介:张方国(1972-),教授,博士生导师,研究兴趣为密码学理论及其应用. Email:isszhfg@mail.sysu.edu.cn

Arithmetic of Elliptic Curves[1]是系统研究椭圆曲线算术理论的一本非常优秀和权威的著作。

椭圆曲线的理论不仅被应用在数学领域，还被广泛应用在计算科学、信息安全、物理学等领域。在1992年出版的 *From Number Theory to Physicsh*[2]一书中，作为讲义形式阐述了一些物理学理论进展所涉及的数论，全书14章的内容就有7章涉及椭圆曲线。Joseph Silverman 教授2007年在 Brown 大学有一个题为“The Ubiquity of Elliptic Curves（椭圆曲线无处不在）”的公开课，主要阐述椭圆曲线的应用，从代数、分析、数论到密码，然后到经典物理（Pendulum 方程）和现代物理（弦理论，场论等）等。此外，椭圆曲线作为构造一类重要的代数几何码－椭圆码的工具，使得它在纠错编码领域也备受重视。

我们将主要关注椭圆曲线在密码中的应用。自从上世纪80年代椭圆曲线被首次应用于密码学领域以来，至今已经有了各种各样的应用。1997年在加拿大滑铁卢举办了第一届椭圆曲线密码学研讨会（ECC workshop），之后该研讨会每年举行一次。ECC 研讨会主要探讨和关注椭圆曲线密码学以及相关领域的研究进展，关于每年的研讨报告和其他详细内容可以访问该研讨会的网页 http://www.eccworkshop.org/。

讲述椭圆曲线及其在密码中的应用的专著目前也已有很多，其中中文专著也有不少，如文献[3-5]等。对于想了解或研究椭圆曲线密码学的读者来说，按照不同阶段，以作者的观点推荐以下几本书：介绍性或科普性的书可以参看《椭圆曲线》（颜松远著）[6]；入门的可以参看 Washington 的[7]或 Smart 等人的书[8]；提高的可以参看 ECC 手册[9]或 Blake 等人的高级 ECC[10]。如果对椭圆曲线密码体制的软硬件实现感兴趣的，建议看一下 Hankerson 等人的 *Guide to Elliptic Curve Cryptography*[11]。

本文主要综述椭圆曲线在密码中的应用，从椭圆曲线最早在密码中的应用开始，一直到最近的一些新应用。从时间上，我们把它分为早期应用、近期应用和新应用。本文的章节安排如下：第1节介绍什么是椭圆曲线以及与之相关的一些计算问题；第2节介绍椭圆曲线在密码中的早期应用，包括整数分解、素性检测和椭圆曲线密码体制等；第3节介绍椭圆曲线在密码中的近期应用，主要讲述基于双线性对的密码体制；第4节介绍椭圆曲线的一些新应用，包括构造 Hash 函数和基于同种的密码体制；最后是对椭圆曲线在密码学中的应用的一个展望和结束语。

1 椭圆曲线及其相关问题

椭圆曲线就是三次平滑代数平面曲线，用代数几何的语言说就是亏格为1的代数曲线。域 F 上的椭圆曲线 E 就是满足下列非奇异的 Weierstrass 方程的所有点 (x,y) 的集合：

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6。$$

当域的特征不为2，3时，Weierstrass 方程可以转化为下面短的形式：

$$y^2 = x^3 + ax + b,$$

其中要求判别式 $\Delta = 4a^3 + 27b^2 \neq 0$。

最早使用“elliptic curve”这个词的是苏格兰诗人 James Thomson（1700-1748）[12]，他在1727年写的纪念牛顿的一首诗“A Poem Sacred to the Memory of Sir Isaac Newton”中这样写到：“He, first of Men, with awful wing pursu'd the comet through the long Elliptic Curve”。因为牛顿在1707年证明了在坐标变换下三次曲线有标准方程：$y^2 = x^3 + ax^2 + bx + c$，即椭圆曲线。

椭圆曲线与椭圆完全不同，因为椭圆方程是一个二次方程。G. C. Fagnano（1682-1766）在计算椭圆的弧长时，导出一个如下的积分：

$$\int \frac{1}{x^3 + ax^2 + bx + c}\mathrm{d}x^{[13]},$$

从而发现了椭圆与椭圆曲线有这么一个联系，这也可以当成为什么把 $y^2 = x^3 + ax^2 + bx + c$ 叫做“椭圆”曲线的一个牵强的理由吧。Gauss、Abel、Jacobi 于19世纪20年代发现椭圆函数与椭圆积分的联系，后来被 Riemann（19世纪50年代）、Weierstrass（1863）和 Poincare（1901）进一步明朗化。

通过切割线法则，可以在椭圆曲线上定义一个群运算，从而使得椭圆曲线上点的全体构成一个加法群。在一个特征不为2，3的域上，这些点在下面定义的加法运算下构成一个 Abelian 群：

群运算的恒等元是 O（称为无穷远点），设 P 和 Q 是椭圆曲线上的两个点，若 $P = O$，则 $-P = O$，且 $P + Q = Q + P = Q$；令 $P = (x_1, y_1)$，$Q = (x_2, y_2)$，则 $-P = (x_1, -y_1)$；如果 $Q \neq -P$，则 $P + Q = (x_3, y_3)$，这里 $x_3 = \mu^2 - x_1 - x_2$，$y_3 = \mu(x_1 - x_3) - y_1$，其中当 $Q \neq P$ 时，$\mu = \dfrac{y_2 - y_1}{x_2 - x_1}$；当 $Q = P$ 时，$\mu = \dfrac{3x_1^2 + a}{2y_1}$。

在特征为2或3的域上，由于椭圆曲线方程形

式不同,使得群运算公式与以上公式略有不同。

当椭圆曲线 E 定义在复数域上时, E 同构于 C/Λ, 这里 Λ 是一个格。在特征 0 的域或无限域上,与椭圆曲线相关的研究问题大多集中在整点、群结构、秩、L- 函数、模函数等领域, 如 Mordell-Weil 有限生成定理、Eichler-Shimura 定理、Birch-Swinnerton-dyer 猜测等。在计算机科学, 特别是密码学中,我们关心的是有限域上的椭圆曲线, 即椭圆曲线的定义域 $F = F_q$(或 GF(q)),这里 q 是一个素数或素数的幂。当椭圆曲线定义在有限域上,那么满足椭圆曲线方程的点就只有有限个,椭圆曲线就是一个有限群。按照 Hasse 定理,F_q 上椭圆曲线的点数介于$[q+1-2\sqrt{q},\ q+1+2\sqrt{q}]$ 之间。

定义在有限域上的椭圆曲线相关的研究问题主要有:(1) 有限域上椭圆曲线点数 #E(F_q) 的计算,即计算椭圆曲线在这个域上的点的个数。1985 年, Schoof[14] 提出了一个计算复杂度是多项式时间的算法,但由于整个算法需要的存储量相当大,所以在具体实现算法时不太可行。之后,Atkin 和 Elkies 对 Schoof 算法进行了一些改进,即 SEA 算法,使得这一算法在实际中实现成为可能;(2) 不同有限域上(素域,二元域,最优扩域等) 及不同形式的曲线(Weierstrass 方程、Legendre 方程、Hessian 方程、Huff 方程、二次曲面交方程、Edwards 方程等) 的快速群运算,如点加公式、倍点公式、标量乘 kP 算法等;(3) 椭圆曲线群上一些困难问题的研究包括椭圆曲线离散对数问题(ECDLP:给定曲线 E 上阶为 n 的点 P,若 Q 是 E 上另一个点,找一个整数 k, $0 \leqslant k \leqslant n-1$, 使得 $Q = kP$)、椭圆曲线 Diffie-Hellman 问题(ECDHP:给定 P, aP, bP,计算 abP)、椭圆曲线决策 Diffie-Hellman 问题(ECDDHP:给定 P, aP, bP, cP,判断是否 $c = ab \bmod n$);(4) 消息嵌入算法,即把任意消息映射到椭圆曲线上的点;(5) 椭圆曲线的同态(同构) 映射、同种、模多项式等等。

2　椭圆曲线在密码中的早期应用

2.1　椭圆曲线整数分解方法

椭圆曲线在密码中最早的应用是荷兰数学家 Hendrik Lenstra 在 1984 年提出的利用椭圆曲线性质分解整数的精妙算法。该算法正式发表在 1987 年的数学年刊上[15]。学术界把 Lenstra 的分解算法称为 ECM(elliptic curve method)。ECM 是当前第三快的整数分解方法,最快的分解算法是一般数域筛法 (GNFS)[16], 其次是多多项式二次筛法 (MPQS)[17]。

ECM 的基本想法:假定要分解整数 $n = pq$,首先把某一椭圆曲线 E 定义在(mod n) 上,即环 Z_n 上。找到 E 的某个点 P,选定一正整数 k,利用点加和倍点公式计算 kP(该计算可以在 $O(\log k)$ 时间内完成)。当 $kP = O$ 时,也就是在计算 kP 时出现了模 n 的不可逆元素,即点加或倍点公式中 μ 的分子与 n 不互素,从而可以分解 n。当 $kP = O$ 时,意味着 k 整除该椭圆曲线定义在 F_p 上的群的阶或定义在 F_q 上的群的阶。所以可以通过随机选曲线和点,使得该曲线在模 p 或 q 时的点数是一些小素数乘积,然后取 $k = B!$(B 是某一预先设定的界),计算 kP。

目前 ECM 的分解记录是 2012 年 8 月 12 日由 Samuel Wagstaff 从 $11^{306}+1$ 中分解出的一个 79 位的因子[18]。ECM 的一个有效实现可见 GMP-ECM project: http://ecm.gforge.inria.fr/。

传统的 ECM 主要是利用 Montgomery[19] 型椭圆曲线来实现的,最近有利用椭圆曲线的其他形式特别是 Edwards 曲线来提高 ECM[20] 速度的。Bos 和 Kleinjung 在 2012 年的亚密会上给出了利用 Edwards 曲线实现 ECM 的详细分析[21]。

ECM 的思想很简单,实际上就是将 pollard 的 "$p-1$" 分解法[22] 推广到椭圆曲线群上。不过这一发现激发了学者们进一步研究椭圆曲线在密码和计算数论中的其他应用。

2.2　椭圆曲线素性检测算法

判定一个整数是不是素数在数论和密码学中都有着重要的应用。目前已知最大的素数是 2013 年 1 月 25 日由美国中央密苏里大学 Curtis Cooper 教授领导的 GIMPS 发现的第 48 个梅森素数 $2^{57,885,161}-1$,有 17425170 位[23]。椭圆曲线素性检测方法(ECPP) 是 1986 年由 Shafi Goldwasser 和 Joe Kilian 提出的一个想法[24],并由 Oliver Atkin 在同年转化成一个算法。之后该算法被许多研究者改进,最有名的是 Oliver Atkin 和 Francois Morain 在 1993 的改进[25]。(一个很重要的改变是利用 CM 方法构造曲线,替换了原来随机选曲线。)

ECPP 的基本过程如下:n 是一正整数, E 是定义在 Z_n 上的椭圆曲线: $y^2 = x^3 + ax + b \pmod n$。$m$ 是一整数。如果存在一个比 $(n^{1/4}+1)^2$ 大的整除 m 的素数 q,并且存在椭圆曲线 E 上的点 P,使得 (1) $mP = O$; (2) $(m/q)P$ 是有定义的且不等于 O。那么 n 就是一个素数。

这一素性测试法可认为是 pocklington 定理[26] 在椭圆曲线上的一个推广。法国计算数论专家

Francois Morain 对 ECPP 在程序设计方面做了精心设计和实现，详见 Morain 的 ECPP 主页[27]。

目前ECPP的检测记录是26,642位LR素数。该素数是利用Morain的软件通过分布式计算，从2011年1月开始，历时3个月，于2011年4月检测出来的。如果这一运算量对应于一个处理器的话，累计时间要超过6年(2255天)。

ECPP是一个概率检测算法，但它是一种零错误概率算法。改进的 Atkin-Morain 算法的计算时间复杂度是 $O(\log^4 n)$，这使得它成为首选的素性检测方法[28]。尽管现在已经有确定性多项式时间素性检测算法，即三个印度人 Agrawal，Kayal 和 Saxena 于2002年发明的 AKS 算法[29]，但他们的算法复杂度是 $O(\log^{12} n)$。Lenstra 和 Pomerance[30] 对 AKS 算法进行改进，使得该确定性算法的运行时间复杂度到了 $O(\log^6 n)$。目前 ECPP 依然是最快和最广泛使用的素性检测方法。当被检测的整数 n 是属于某一特殊形式的整数序列时，Abatzoglou 等人[31] 最近改进椭圆曲线素性检测算法，给出了一个确定性的算法，其复杂度仅为 $O(\log^2 n)$。

2.3 椭圆曲线密码体制

1985年，华盛顿大学的 Neal Koblitz[32] 和 IBM 的 Victor Miller[33] 分别独立地提出了利用有限域上椭圆曲线群来设计公钥加密方案，即椭圆曲线公钥密码(elliptic curve cryptography，ECC)。从体制上说，ECC 并没有给出任何新的方案，它只是提供了一个实现传统 DLP 体制的新的载体，就是将原来基于有限域的乘法循环子群的密码方案平移到有限域的椭圆曲线群上来。给定椭圆曲线密码体制的参数，如有限域、曲线、群的阶、生成元等，那么基于椭圆曲线的加密、签名、密钥协商等协议都可以由现有的那些基于一般离散对数的方案转化过来，如 Diffie-Hellman 密钥协商协议变成 ECDH，MQV 变成 ECMQV，ElGamal 加密方案变成 EC-ElGamal，DSA 变成 ECDSA 等。

ECC 在与基于乘法群的密码体制和 RSA 体制相比具有无可比拟的优势。由于 ECC 具有的特性，在同等安全强度下，与其他体制相比，ECC 可以用较小的开销(所需的计算量、存储量、带宽、软件和硬件实现的规模等)和时延(加密和签名速度高)实现较高的安全性，因此，ECC 特别适用于计算能力和集成电路空间受限(如 Smart 卡)、带宽受限(如无线通信和某些计算机网络)、要求高速实现的情况。正因如此，ECC 从一提出就受到了国际上的广泛关注。

经过近30年的研究，ECC 目前的理论已经非常成熟，并且早已走向实用。当前在 ECC 方面的研究主要集中在以下几个方面：

(1) 更快速实现：椭圆曲线密码体制的实现涉及有限域的基本运算，椭圆曲线点加、倍点和标量乘等。任何一方面的提速都会改进椭圆曲线密码体制实现效率。尽管目前 ECC 的软硬件实现已经足以实用，但仍有很多学者还在精益求精地改进 ECC 的运算算法，从而一点点地提高 ECC 软硬件实现速度。椭圆曲线的不同形式使得椭圆曲线的群运算公式有所不同。Montgomery 曲线[19] 和 Edwards 曲线[34] 上的群运算不仅比传统的 Weierstrass 曲线有效，并且还可以抗击简单的能量攻击(SPA)。特别地，对 Edwards 曲线及其变形的研究近几年在椭圆曲线算术方面比较热[35-37]。

另外，在探索椭圆曲线新的同态以及利用它进行快速标量乘方面也有几个很有意义的工作，如 Galbraith-Lin-Scott 在欧密会 2009 上对定义在 $GF(q^2)$ 上的一大类椭圆曲线构造了新的自同态[38]，Hankerson 等人[39] 将 Galbraith 等人的方法推广到了二元域上。

(2) 标准化与新产品：在椭圆曲线密码体制的标准化方面，IEEE、RSA，NIST、ISO、IETF、ATM 等都作了大量的工作，它们所开发的椭圆曲线标准的文档有 IEEE P1363 P1363a、PKC#13、ANSI X9.62 X9.63、ISO/IEC18033-2、SECG SEC1 等。除美国和加拿大外，日本、欧洲、韩国和俄罗斯等也在纷纷进行 ECC 技术研发，并推出了一些重要成果或 ECC 标准(如日本的 PSEC、韩国的 EC-KDSA 和欧洲的 NESSIE)等。加拿大 Certicom 是 ECC 的主要商业支持者，是在商界探索如何高效、安全、低成本来实现和推广 ECC 技术和产品的最早的公司。从1997年开始，全球各大公司和机构开始竞相采用 Certicom 的 ECC 技术或与之建立战略联盟。Certicom 公司拥有一系列的 ECC 核心技术，目前已经拥有和正在申请的 ECC 专利超过300项，这些专利涵盖 ECC 安全优化和安全实现的所有领域。由于 RFID 技术的发展及其广泛应用，研究椭圆曲线在 RFID 上的应用和实现的工作也有很多。

我国在 ECC 的标准化和产业化方面做了很多工作：2003年5月12日中国颁布的无线局域网国家标准 GB15629.11 中，包含了全新的 WAPI(WLAN authentication and privacy infrastructure)安全机制，能为用户的 WLAN 系统提供全面的安全保护。WAPI 中采用的公钥密码体制就是椭圆曲线算法。

2012 年 3 月 21 日,国家密码管理局颁布了 6 项密码行业标准,其中包括椭圆曲线密码算法标准,即 GM/T0003-2012《SM2 椭圆曲线公钥密码算法》。在该标准中,规定了 SM2 椭圆曲线公钥密码算法的数字签名算法、密钥交换协议、公钥加密算法和曲线参数,并给出了数字签名与验证、密钥交换与验证、消息加解密示例。截止2012 年12 月31 日,支持SM2 椭圆曲线密码算法的通用产品已达 266 项[40]。椭圆曲线也被广泛应用在可信计算中,国家密码管理局 2007 年12 月颁布的《可信计算密码支撑平台功能与接口规范》中,规定所用公钥密码算法就是椭圆曲线密码算法。

(3) 安全性方面的研究:安全性是任何一个密码体制的核心问题,ECC 是建立在求椭圆曲线离散对数(ECDLP) 困难基础之上的。目前除了对一些特殊曲线上的离散对数能有效计算外,对所有曲线上的离散对数还没有有效的算法。

存在的对特殊曲线的攻击主要有:

Pohlig-Hellman 攻击[41] —— 适用于光滑阶的曲线,所以为了抗击这种攻击,椭圆曲线群的阶必须有大素因子;

Smart-Satoh-Araki-Semaev 攻击[42-44] —— 适用于非正规曲线(即 $\#E(F_q) = q$),该算法可以将 $E(F_q)$ 上的 ECDLP 规约到加法群 F_q 上的 DLP;

MOV-Frey-Rck 攻击[45-46] —— 适用于嵌入次数较小的椭圆曲线,即 $\#E(F_q)$ 整除 $q^k - 1$,k 比较小时,利用双线性对将ECDLP 规约到有限域的扩域上的 DLP(当椭圆曲线和有限域的乘法群中的 DLP 都困难时,可用来构造密码方案,即基于双线性对的密码体制。);

Weil Descent 或GHS 攻击[47-48] ——适用于扩域曲线,通过 Weil 下降的思想将扩域上椭圆曲线 $E(F_{q^n})$ 的 DLP 规约到子域高亏格代数簇 $\mathrm{Jac}(C)(F_q)$ 上的 DLP,然后用指标计算法求解它。

Lauter 和 Stange 在文献[49] 中还讨论了椭圆除序列或椭圆网与ECDLP 的关系。由于椭圆除序列和 Weil 对都与椭圆曲线的 Weierstrass σ 函数有关,所以这个方法本质与 MOV 攻击等价。

使用 F_p 和 $\mathrm{GF}(2^m)$(m 是素数) 上随机椭圆曲线的充分大素数阶子群(现在要求 160 比特以上)就可以防止以上特殊曲线的攻击。目前的所有工业标准都是使用这两类曲线。对于这两类曲线或更一般的曲线上的离散对数来说,目前最好的攻击算法是利用生日悖论原理设计的 Pollard rho 算法[50] 和它的并行变形算法[51],它们的计算复杂度是指数级的。

1997 年,加拿大 Certicom 公司为了鼓励对 ECC 的研究以及评估其安全性,开展了 Certicom ECC 挑战项目[52]。该挑战分为 3 类:一些相对容易解决的实验(79bit, 89bit, 97bit);第 I 级的挑战(109bit, 131bit);第 II 级的挑战(163/191/239/359bits)。对每一种类型有三种形式的曲线:a) 素域上的素数阶随机椭圆曲线(ECCp); b) 二元域上有大素数阶子群的随机椭圆曲线(ECC2); c) 二元域上有大素数阶子群的 Koblitz 椭圆曲线(ECC2K)。随后从 ECC2-79 到 ECCp-109 已逐步被破解。Daniel V. Bailey 等人[53] 组成的全球性研究团队正在挑战 ECC2K-130,并有望在 2013 年内取得成功,有兴趣的读者可以访问网站 http://ecc-challenge.info/ 获得该工作的最新进展。目前攻击ECDLP 的世界纪录是 Joppe W. Bos 等人[54] 破解的 112 比特的 ECDLP:2009 年 7 月,瑞士洛桑联邦理工学院(EPFL) 的密码算法实验室使用 200 多台 PS 3 游戏机组成的集群,耗时近 6 个月,破解素数域上 112 比特ECDLP。攻击的曲线是SEC 标准中推荐的最低安全度的曲线 secp112r1。所用的方法就是 Pollard rho 并行算法。

ECDLP 是一块硬骨头,寻找计算 ECDLP 的新算法是公认的难题。最近几年在求解ECDLP 的理论研究的工作主要体现在两个方面:一是 Pollard rho 和它的并行变形的改进。韩国首尔大学的 Cheon 教授[55] 研究了带有辅助输入的离散对数问题的求解,并将它应用到强 Diffie-Hellman 问题(q-SDHP) 上去。张等人[56] 利用"二元域上椭圆曲线的半点比倍点快" 这一事实,提出了提高二元域上 ECDLP 计算的算法,对于美国 NIST 推荐的二元扩域 $\mathrm{GF}(2^{233})$ 上的随机曲线,新的算法比以前最好的算法快约 12% ~ 17%。

ECDLP 的另一方面的研究就是寻求指标计算(Index Calculus) 及其他亚指数时间算法的努力。一般有限域乘法群上的离散对数有亚指数时间算法攻击 —— 指标计算法,但这种方法不能应用到 ECDLP 上,因为在指标计算法中找一组因子基是很基本的,椭圆曲线点群上目前找不到有效因子基。早在 1998 年 Silverman[57] 就提出了一个新的攻击方法:Xedni 计算法,该方法主要是把有限域上的曲线提升为有理数域上的曲线,在有理数域上利用点的高度(Height) 计算离散对数问题。根据 Koblitz 等人[58] 的讨论,Xedni 计算法成功的概率是非常小的,且它的计算量仍是指数时间的。2004 年,Semaev[59] 提出了椭圆曲线的聚合多项式,并用求

解该多项式的比较小的根来构造因子基。Gaudry[60]将 Semaev 的聚合多项式方法应用在扩域曲线上，结合 Weil Descent 方法，给出了一个 GF(q^n) 上的当 $n \geqslant 3$ 时的 ECDLP 比 Pollard rho 方法快的算法。Diem[61] 扩展了 Gaudry 的方法，并证明了该算法是亚指数时间复杂度的。Joux 等人[62] 将 Gaudry 和 Diem 的算法应用在 GF(q^6) 的 ECDLP 上，并计算了一个 149 比特的具体例子。Faugère 等人[63] 在 2012 欧密会上将 Gaudry 和 Diem 的算法应用在 GF(2^n) 上，证明了如果关于 Groebner 基的某个猜测正确的话，GF(2^n) 上的 ECDLP 有亚指数时间攻击。但是目前 n 需要上千比特以上，这个亚指数时间算法才显出优势（相比 Pollard rho 算法）。

Cheng 在文献[64] 中把 ECDLP 规约到计算一个代数几何码的最小汉明重量的码字问题上。计算一个随机代数几何码的最小汉明重量的码字是一个 NPC 问题，任何 NP 都可以规约到这个问题，ECDLP 是一个 NP 问题，自然可以规约到这个 NPC 问题上来。Cheng 利用了 Riemann-Roch 理论，使得这个规约非常紧致有效。

近年来，借助侧信道所泄漏的信息，如计算需要的时间、计算能量消耗等等对密码协议实施攻击的各种侧信道攻击方法被提出。这些侧信道攻击也可以用在椭圆曲线密码体制中。关于 ECC 中的各种侧信道攻击及其预防技术可以参见文献[10] 的第4、5章或文献[9] 的第 29 章。

2.4 在一些困难问题的等价性证明中的应用

椭圆曲线在密码中的早期应用还体现在利用椭圆曲线辅助证明密码中的一些困难问题的等价性。对于一个阶为素数 q 的循环群 $G = \langle g \rangle$，有两个重要的问题。一个是 DLP：已知 g, g^x 求 x；另一个是 CDHP：已知 g, g^a, g^b，求 g^{ab}。如果 DLP 可解，那么 CDHP 显然可解。但反过来却不容易推导。1994 年，Maurer[65] 借助于有限域上椭圆曲线给出了一个非常巧妙的证明。Maurer 证明了对于群的阶 q，如果在有限域 GF(q) 上可以找到光滑的阶（这个阶的最大素因子是 $O(\log^a q)$ 的数量级）的椭圆曲线，则 DLP 和 CDHP 多项式时间等价。尽管目前还没有多项式时间算法构造给定有限域上的光滑的阶的椭圆曲线，但利用 Maurer 的方法可以证明一些公开的密码标准中的循环群中 DLP 和 CDHP 是等价的[66]。

3 椭圆曲线在密码中的近期应用

3.1 基于双线性对的密码体制

椭圆曲线或超椭圆曲线的双线性对一般是指 Weil 对和 Tate 对。双线性对在密码中的应用最早归于 Menezes，Okamoto 和 Vanstone 以及 Frey 和 Rück 的工作，即著名的 ECDLP 的 MOV 攻击[45] 和 FR 攻击[46]。2000 年，Sakai 等人[67] 和 Joux[68] 同时发现了双线性对在密码中的正面的应用——能够用来构造新的密码方案。之后，特别是 2001 年 Boneh 和 Franklin[69] 利用双线性对实现了基于身份的加密，双线性对引起了密码学家们的极大兴趣，在密码中又被发现了更多各种各样的应用。

什么是双线性对呢？令 G_1, G_2 和 G_T 是三个 q 阶循环群，我们考虑 G_1, G_2 中的群运算是加法，G_T 是乘法群。一个双线性对 e 就是一个从 $G_1 \times G_2$ 到 G_T 的映射，并满足如下性质：1）双线性性：设 $P \in G_1$，$Q \in G_2$，$a, b \in Z_q$，有 $e(aP, bQ) = e(P, Q)^{ab}$；2）非退化性：对每一个 $P \in G_1 / \{1\}$，总存在 $Q \in G_2$，使得 $e(P, Q) \neq 1$；3）有效可计算性。利用椭圆曲线构造的双线性对有下面三种类型：类型 1，$G_1 \rightarrow G_2$ 有一个有效可计算的同构，这时一般可假定 $G_1 = G_2$；类型 2，$G_2 \rightarrow G_1$ 有一个单向同构；类型 3，没有任何 $G_1 \rightarrow G_2$ 或 $G_2 \rightarrow G_1$ 的有效可计算的同构。

双线性对在密码构造中的一个重要应用是实现基于身份的加密。Boneh-Franklin 的 IBE 在随机预言（random oracle，RO）模型下被证明是 IND-ID-CCA 的。Waters 在 Eurocrypt 2005 上[70] 给出了一个有效的在标准模型下可证明安全的基于身份的加密方案。在基于身份的密码体制中，用户的公钥可以是任何惟一识别用户身份的任何信息，如身份证号、email 地址、驾驶证号等等，当然可以惟一识别用户的一些生物特征也自然可以作为基于身份的公钥体制中的用户公钥。然而由于生物特征具有非精确再生性，即同一个生物特征的两个测量值不完全相同，所以将生物特征作为公钥信息时，就带有了模糊性。Sahai 和 Waters[71] 在对 IBE 和生物特征进行了研究后，提出了基于模糊身份的加密体制（FIBE）。由于生物特征信息看成是具有某些特定属性的一个集合，Sahai 和 Waters 将基于模糊身份的加密体制加以简单推广，得到了基于属性的加密体制（ABE）。基于属性的加密体制有两种方法可以用在接入控制结构的设计中，它们分别是密钥策略（Key-Policy）ABE 和密文（Ciphertext-Policy）策略 ABE。断言加密（Predicate encryption）[72] 是基于身份的加密的一个推广，密钥对应于一个断言 f，密文关联着一些属性，对应于断言 f 的密钥 SKf 能够用来解密具有属性 I 的密文当且仅当 $f(\mathrm{I}) = 1$。Boneh 和 Hamburg 在 Asiacrypt 2008 上给出了广义的基于身份的加密（GIBE）的概念[73]。一个广义的基于身

份的加密方案,允许一些策略的参与来进行加密信息,这些策略来自一些允许的策略集合 P。由于基于属性的加密可以在云存储中实现高效、精细、灵活的密文访问控制,所以基于身份的密码体制在云计算领域有了重要应用。

双线性对在密码构造中另一个重要应用是构造短签名,短的数字签名在某些环境下特别是通信带宽受限制的情况下是需要的。目前利用双线性对构造的短签名方案主要有三个,这些短签名方案同时也是很多其他基于双线性对密码协议的设计基础。第一个利用双线性对构造的短签名是 Boneh 等人[74]2001 年提出的 BLS 方案,它的构造和安全性是基于 CDHP。BLS 签名需要一个特殊 Hash 函数,即将任意消息 Hash 到椭圆曲线上的点(消息嵌入编码)。在 2007 年之前,到任意椭圆曲线上的消息嵌入都是概率算法。2007 年美密会上,Icart[75] 提出了一个确定性多项式时间算法。2004 年 PKC 上,张等人[76]提出了第二个基于双线性对的短签名方案 ZSS04,同年 Boneh 和 Boyen[77] 在欧密会上给出了标准模型下安全的构造 BB04。ZSS04 和 BB04 的构造和安全性是基于 Inv-CDHP(即给定 P, aP 求 $a^{-1}P$),这个问题与 CDHP 等价。ZSS04 和 BB04 方案比 BLS 方案有效,且不需要特殊 Hash 函数。在 2006 年的越南密码会上张等人[78]基于计算指数平方根问题(CSREP,即给定 P, aP,求 $a^{1/2}P$)提出了 ZCSM06 方案。对于计算指数平方根问题的困难性,张[79]证明了当群的阶是某种特殊的素数时,CSREP 与平方 CDHP 等价,从而与 CDHP 等价。Roh 等人[80] 证明了在大多数情况下 CSREP 与 CDHP 等价。

基于双线性对的密码体制已经被研究了十多年,并有了非常多的研究成果。当前对这一领域的研究主要集中在以下几个方面:

(1)新密码方案的构造。利用双线性对设计的密码方案,要么这些方案是非常困难甚至不可能用其他的传统数学问题如离散对数或 RSA 问题来设计;要么虽然可以用其他的数学问题来实现,但是非常复杂以至于不实用。经过这么多年的设计,容易设计的密码方案基本都设计出来了。在密码设计方面,需要探求更新奇更巧妙的方案。

(2)新的双线性对和适用于双线性对的椭圆曲线的构造。最早用于设计密码体制的双线性对是超奇异椭圆曲线的 Weil 对和 Tate 对。由于大多数情况下计算 Tate 对比计算 Weil 对要有效得多,所以双线性对的实现大都关注 Tate 对及其一些有效变形。实现双线性对的主要算法是利用 Miller 算法[81],目前提出的许多改进算法也都是基于 Miller 算法的。影响双线性对快速实现的因素很多,其中一个很重要的因素就是 Miller 算法中的循环次数:循环次数越少,计算速度越快。围绕如何减少Miller 算法中的循环次数,提出了一些新的双线性对,从最初的 Tate 对,到 Eta 对[82],Ate 对[83],广义的 Ate 对[84],Rate 对[85],一直到最优对[86]。构造适用于双线性对的椭圆曲线主要是利用 CM 方法。在素数域上已经利用 CM 方法构造出了大量适用于各种双线性对的椭圆曲线,但在二元域上,目前还没有有效的方法构造适用于双线性对的非超奇异椭圆曲线。

(3)双线性对的快速实现。目前双线性的计算已经非常有效。下面是 128 比特安全性的双线性对(相当于256 比特的 ECC 和3000 比特的 RSA)利用 BN 曲线实现的时间竞赛:2007 年的双线性对会议上,Devigili 等人[87]在 32-bit Intel Pentium IV @ 3.0 GHz 的机器上的实现用了 23 ms;2008 年,Grabher, Groβschädl, Page[88] 在 64-bit Intel Core 2 Duo @ 2.4 GHz 的机器上用了 6 ms;同年,Hankerson, Menezes, Scott[89] 在与 Grabher 等人相同的机器上的实现只用了 4.2 ms;2010 年,Naehrig 等人[90] 在 64-bit Intel Core 2 Duo @ 2.8 GHz 机器上的实现用了 1.5 ms,Beuchat 等人[91] 对 254 比特 BN 曲线上的最优 Ate 对在 64-bit Intel Core i7 @ 2.8 GHz 机器上的实现用了 0.8 ms。目前对这一安全级别的双线性对的实现的最好记录是 2011 年 Aranha 等人[92] 在欧密会上的结果:0.56 ms(64-bit AMD Phenom II @ 3.0 GHz)。

(4)双线性对密码体制的标准化与产品。近几年,基于双线性对的密码体制,特别是基于身份的密码体制在工业界已经有了许多应用实例。随着应用的逐渐广泛,国际上许多标准组织也在积极地进行这一密码体制的标准化工作。2006 年,国际标准化组织 ISO 在 ISO/IEC 14888-3 中给出了两个利用双线性对设计的基于身份的签名体制的标准;IEEE 也组织了专门的基于身份的密码体制的工作组(IEEE P1363.3)。2007 年 8 月,NIST 也在着手制定基于身份的密码体制和基于双线性对的密码体制的标准。我国也已经启动了基于身份的密码体制的标准化工作,并已经取得了一些进展。

(5)双线性对密码体制的安全性研究。如果双线性对群 G_1,G_2 或 G_T 中的离散对数可解,那么基于双线性对的密码体制是显然不安全的。多数基于双线性对的密码体制实际上基于比 DLP 还弱一点的问题:双线性对逆问题(BPI),即给定 P, $e(P, X)=a$,去计算 X。Galbraith 等人在文献[93]中对

双线性对逆问题给出了一个框架性的论述。对于双线性对密码体制的实际攻击,最近日本信息通信研究机构(NICT)、九州大学和富士通公司[94],利用21台通用计算机(252核)在148.2天内利用函数域筛法成功地计算了有限域GF(3^{6*97})上的离散对数,从而破解了定义在GF(3^{97})上的超奇异椭圆曲线的278比特的双线性对。这一工作创造了破解双线性对密码的新的世界记录。

3.2 伪随机函数与流密码

椭圆曲线在密码中的近期应用还体现在设计伪随机数(序列)产生器和构造好的密码性质的布尔函数。NIST在2006年颁布了椭圆曲线随机数生成器(ECRNG)算法标准,即NIST SP 800-90。Brown等人[95]在2007年的美密会上对这一算法的安全性进行了分析并得出如下结论:如果椭圆曲线的DDH问题、x-对数问题和截断点问题是困难的,那么ECRNG是安全的。

有限域上伪随机序列发生器可以推广到椭圆曲线上。由于椭圆曲线理论丰富,使得椭圆曲线伪随机序列的构造方法更加多样化,同时由于椭圆曲线诸多的代数特性,使得这些新伪随机序列具有许多很好的密码性质,如分布一致性,相关性,线性复杂度等。Gong等人[96]利用迹函数,把椭圆曲线上的点作用到二元域,从而给出了三种不同的构造椭圆曲线序列的方法,并利用椭圆曲线的性质分析了这些序列的周期,线性复杂度和0-1分布。Beelen等人[97]推广了Gong等人的方法,分别利用椭圆曲线的加法特征和乘法特征来构造伪随机序列。

弹性函数即平衡的相关免疫布尔函数,其在流密码体制中的非线性组合模型中有着很重要的应用。Cheon等人[98]给出了两个多项式型的布尔函数之间的相关性与代数曲线的点数的关系,并通过这个关系,利用椭圆曲线提出了一个构造弹性函数的方法。

4 椭圆曲线在密码中的一些新应用

最近几年,椭圆曲线在密码中又被发现了一些新的有趣的应用,主要体现在构造Hash函数和基于同种的密码体制。

4.1 构造Hash

2008年,Brown等人[99]利用二元域上椭圆曲线设计了一个有效的椭圆曲线Hash函数(ECOH),并提交NIST的SHA-3候选标准。但非常不幸的是最初的算法由于被发现有第二原像攻击而被淘汰。通过增大椭圆曲线的规模或其他简单修正得到的ECOH2,可以防止第二原像攻击。ECOH的构造是基于MuHASH(即Hash的运算是一个群中的乘法)模式的。MuHASH是可证明安全的,其安全性是基于群中的离散对数问题,但MuHASH实际使用效率太低。ECOH主要应用二元域上椭圆曲线运算和填充功能,使得实现效率大大提高。另外ECOH没有像MuHASH那样使用随机预言,所以它的安全性尽管与ECDLP相关,但没有严格给出证明。

最近,Omar等人[100]利用椭圆曲线的L-函数构造了一个单向函数,并给出一个新的Hash函数的构造。

4.2 基于同种的密码体制

椭圆曲线的同种(或同源)isogeny是两条椭圆曲线之间的一个非平凡代数映射,它是一个群同态。具体地,设E_1, E_2是定义在域F上的两条椭圆曲线,一个同种ϕ: $E_1 \to E_2$就是形如$\phi(x,y) = (\frac{f_1(x,y)}{g_1(x,y)}, \frac{f_2(x,y)}{g_2(x,y)})$的一个同态映射。同种$\phi$的次数就是代数映射的次数。关于有限域上椭圆曲线同种的结论,有下面著名的Tate的同种定理(Tate's Isogeny Theorem):

有限域F_q上的两条椭圆曲线E_1, E_2, 如果$\#E_1(F_q) = \#E_1(F_q)$,则存在一个同种映射ϕ: $E_1 \to E_2$。

椭圆曲线的同种问题就是给定有限域F_q上的两条相同点数的椭圆曲线E_1, E_2,找这样的一个同种映射。

同种问题有多么难呢?对于一般(ordinary)椭圆曲线,同种问题最快的算法是由Galbraith,Hess和Smart[101]在2002年提出的GHS算法,其时间复杂度是$O(\sqrt[4]{q})$。对于超奇异(supersingular)椭圆曲线,同种问题目前最快的算法是由Jao等人[102]给出的,其时间复杂度是$O(\sqrt{q})$。同种问题被普遍认为是抗量子计算的!Childs,Jao和Soukharev[103]研究了同种问题的量子算法,没有找到量子计算机下的多项式时间算法,他们只找到了一个亚指数时间算法。

低次同种有明确的计算公式,可有效计算,如$E_1: y^2 = x^3 + ux^2 + 16ux$到$E_2: y^2 = x^3 - 2ux^2 + u(u - 64)x$有一个二次同种$\phi(x,y) = (\frac{x^2 + ux + 16u}{x}, \frac{yx^2 - 16uy}{x^2})$。利用低次同种可以构造一个同种图$G = (V,E)$:它的顶点代表在一个给定的层次所有的椭圆曲线,而其边代表低次同种。如果有边(E_1, E_2),当且仅当E_1和E_2是低次同种的椭圆曲线。同种图是扩展图(Expanders)。

同种(特别是低次同种)早期被应用在有限域上椭圆曲线点数计算算法(如 SEA[104]),提高标量乘算法[105]和攻击 ECDLP(如提速 Weil decent 攻击[101])或分析相同定义域上同阶 ECDLP 的等价难度等[106]。近几年被发现可以用来构造密码方案。

Charles 等人[107]在 2009 年提出了利用扩展图构造可证明安全的 Hash 函数的方法,作为一个具体例子,他们利用 GF(p^2)上的超奇异椭圆曲线同种图给出了一个实现。如果要 Hash 的消息是 $m_0m_1\cdots m_{k-1}$,在同种图上从一条给定的曲线 E 出发,用 m_i 决定向左还是向右走的每一步,最后达到的曲线就是 Hash 值 $H(m_0m_1\cdots m_{k-1})$。

在一个同种图上,两条路径 R_A 和 R_B 满足性质 $R_A(R_B(E)) = R_B(R_A(E))$。基于这个事实,Rostovtsev 和 Stolbunov[108]提出了一个基于同种的密钥交换协议,该协议就是 Diffie-Hellman 密钥协商协议的同种模拟:Alice 和 Bob 的公共参数是同种图和图上一顶点 E。Alice 选择一个秘密路径 R_A,将 $R_A(E)$发给 Bob;Bob 选择一个秘密路径 R_B,将 $R_B(E)$发给 Alice。Alice 可以计算 $R_A(R_B(E))$,Bob 可以计算 $R_B(R_A(E))$,所以他们得到相同的一个顶点,从而作为协商的秘密。有了基于同种的 Diffie-Hellman 密钥协商协议就可以给出基于同种的 ElGamal 加密。

Stolbunov 提出的基于同种的加密方案是利用一般曲线的同种来构造的。对于 128 比特安全强度的系统,选取的椭圆曲线是定义在 428 比特的有限域上的,Stolbunov 在文献[109]中给出的实现是 229 s。Jao 等人[110]利用超奇异椭圆曲线的同种构造了更加有效的密钥协商和公钥加密方案,他们给出的 1024 比特有限域上的同种密码加密的实现是 500 ms(64 位 2.4GHz 处理器)。

目前基于同种的签名方案还没有提出。

5　展望与结束语

基于椭圆曲线离散对数的密码体制,基于双线性对的密码体制,基于同种的密码体制,我们把这些利用椭圆曲线来设计的密码体制统称为椭圆曲线密码体制,或广义的椭圆曲线密码体制。

在密码学领域是最难做预言或展望的,因为在密码中可以说是没有什么不可能的,就像李宁或 adidas 的广告语“Anything is possible”,“Impossible is nothing”。没有人敢说自己设计的密码体制是永远安全的。椭圆曲线密码体制也不能说就是永远安全的。目前已经存在的椭圆曲线密码体制的安全性主要依赖于 ECDLP 或同种问题。

我们可以简单地探讨一下椭圆曲线密码体制的前景。如果是乐观的考虑的话,ECDLP 可以一直扛到量子计算机实用化,或同种问题不存在多项式时间的量子算法。如果悲观地考虑的话,ECDLP 可能在将来被发现了多项式时间算法,或者找到了同种问题的多项式时间的量子算法。ECDLP 是属于 NP 类的,目前从理论上证明 ECDLP 不属于 P 问题类,即不存在多项式时间求解算法似乎是不太可能。因为如果可能,就意味着证明了 $P \neq NP$。而 P 和 NP 的关系是计算复杂性理论中的核心问题,至今没有解决。从这种逻辑上讲,ECDLP 可能会有多项式时间算法的。如果真是这样的话,ECDLP 的解决算法可能会是这样的,要么是一种初等的办法,这是因为椭圆曲线的运算涉及的方面太多,也许某个或某些地方能暴露出它的致命缺陷。但这一般需要天才的技巧;要么是高等的,可能需要更高深的数学知识,这是因为椭圆曲线的理论太丰富,需要探求它更深层次的性质才能解决它。

椭圆曲线是亏格为 1 的超椭圆曲线,椭圆曲线的这些密码应用大都可以推广到超椭圆曲线上去,如超椭圆曲线密码体制、超椭圆曲线素性检测、超椭圆曲线双线性对、超椭圆曲线的同种的构造与计算等等。由于超椭圆曲线比椭圆曲线具有更丰富的代数结构,有更多的工具用来设计新的应用,所以对超椭圆曲线在密码中的应用研究非常值得关注。

致谢:本文是根据第六届中国可信计算和信息安全会议上的邀请报告整理而成的。作者在此对会议的组织者和举办者表示感谢!

参考文献:

[1] SILVERMAN J H. The arithmetic of elliptic curves[M]. New York:Springer-Verlag, 1986.

[2] WALDSCHMIDT M, MOUSSA P, LUCK J-M, et al. From number theory to physics [M]. New York: Springer Press, 2001.

[3] 裴定一,祝跃飞. 算术数论[M]. 北京:科学出版社,2002.

[4] 王学理,裴定一. 椭圆与超椭圆曲线公钥密码的理论与实现[M]. 北京:科学出版社,2006.

[5] 祝跃飞,张亚娟. 椭圆曲线公钥密码导引[M]. 北京:科学出版社,2006.

[6] 颜松远. 椭圆曲线[M]. 大连:大连理工大学出版社,2011.

[7] WASHINGTON L. Elliptic curves: number theory and cryptography [M]. Chapman & Hall:CRC Press, 2003.

[8] BAKE I F, SEROUSSI G, SMART N. Elliptic curve in cryptography [M]. London: Cambridge University

Press, 1999.

[9] COHEN H, FREY G, AVANZI R, et al. Handbook of elliptic and hyperelliptic curve cryptography[M]. London: CRC Press, 2005:34.

[10] BAKE I F, SEROUSSI G, SMART N. Advances in elliptic curve cryptography[M]. Cambridge: Cambridge University Press, 2005.

[11] HANKERSON D, MENEZES A, VANSTONE S. Guide to elliptic curve cryptography[M]. New York: Springer, 2003.

[12] Florian Heβ, Andreas Stein, Sandra Stein, et al. The magic of elliptic curves and public-key cryptography[J]. Jahresbericht der Deutschen Mathematiker-Vereinigung, 2012, 114(2):59-88.

[13] BROWN E. Three Fermat trials to elliptic curves [J]. The College Mathematics Journal, 2000, 31:162-172.

[14] SCHOOF R. Elliptic curves over finite fields and the computation of square root mod p [J]. Mathematics of Computation, 1985(44):483-494.

[15] LENSTRA Jr H W. Factoring integers with elliptic curves [J]. Annals of Mathematics, 1987, 126(3): 649-673.

[16] LENSTRA A K, LENSTRA Jr H W. The development of the number field sieve [M]. New York: Springer, 1993:1554.

[17] POMERANCE C, SMITH J W, TULER R. A pipeline architecture for factoring large integers with the quadratic sieve algorithm[J]. SIAM J Comput, 1988, 17:387-403.

[18] http://www.loria.fr/~zimmerma/records/top50.html?

[19] MONTGOMERY P L. Speeding the pollard and elliptic curve methods of factorization [J]. Mathematics of Computation, 1987, 48(177):243-264.

[20] BERNSTEIN D J, BIRKNER P, LANGE T, et al. ECM using edwards curves [J]. Mathematics of Computation, 2013, 82:1139-1179.

[21] JOPPE W BOS, THORSTEN Kleinjung. ECM at work [C]//Proceedings of ASIACRYPT. Berlin: Springer-Verlag, 2012, 7658:467-484.

[22] POLLARD J M. Theorems on factorization and primality testing [J]. Proceedings of the Cambridge Philosophical Society, 1974, 76:521-528.

[23] GIMPS project discovers largest known prime number, $2^{57,885,161}-1$ [EB/OL]. [2013-01-02]. http://www.mersenne.org/various/57885161.htm

[24] GOLDWASSER S, KILIAN J. Almost all primes can be quickly certified[C]//Proceedings of the Eighteenth Annual ACM Symposium on the Theory of Computing. New York: ACM Press, 1986:316-329.

[25] ATKIN A O L, MORAIN F. Elliptic curves and primality proving [J]. Mathematics of Computation, 1993, 61:29-68.

[26] The ECPP home page[EB/OL]. [2013-01-02]. http://www.lix.polytechnique.fr/~morain/Prgms/ecpp.english.html

[27] WEISSTEIN, ERIC W. Pocklington's Theorem. [EB/OL]. [2013-02-02]. http://mathworld.wolfram.com/PocklingtonsTheorem.html.

[28] MORAIN F. Implementing the asymptotically fast version of the elliptic curve primality proving algorithm[J]. Mathematics of Computation, 2007, 76:493-505.

[29] AGRAWAL M, KAYAL N, SAXENA N. PRIMES IS IN P [J]. ANNALS OF MATH, 2004, 160:781-793.

[30] LENSTRA JR H W, Pomerance Carl. Primality testing with Gaussian periods[EB/OL]. [2013-01-26]. http://www.math.dartmouth.edu/~carlp/aks041411.pdf, 2011.

[31] ABATZOGLOU A, SILVERBERG A, SUTHERLAND A V, et al. Deterministic elliptic curve primality proving for a special sequence of numbers[EB/OL]. [2013-02-15]. http://math.ucsd.edu/~kedlaya/ants10/abatzoglou/paper.pdf.

[32] KOBLITZ N. Elliptic curve cryptosystems[J]. Mathematics of Computation, 1987, 148(177):203-209.

[33] MILLER V. Uses of elliptic curves in cryptography [C]//Proceeding of Lecture notes in Computer Sciences. New York: Springer-Verlag New York, Inc, 1986:417-426.

[34] EDWARDS H M. A normal form for elliptic curves[J]. Bull Amer Math Soc, 2007, 44(3):393-422.

[35] BERNSTEIN D J, BIRKNER P, LANGE T. et al. Twisted Edwards curves [J]. Africacrypt, 2008, 5023: 389-405.

[36] BERNSTEIN D J, LANGE T. Faster addition and doubling on elliptic curves[J]. Asiacrypt, 2007, 4833:29-50.

[37] BERNSTEIN D J, LANGE T, FARASHAHI R. Binary Edwards curves[C]//Proceeding sof the 10th international workshop on Cryptographic Hardware and Embedded Systems. Berlin-Heidelberg: Springer-Verlag, 2008, 5154:244-265.

[38] GALBRAITH S, LIN Xibin, SCOTT M. Endomorphisms for faster elliptic curve cryptography on a large class of curves [C]//Proceedings of EUROCRYPT. Berlin-Heidelberg: Springer-Verlag, 2009: 518-535, 2009

[39] HANKERSON D, KARABINA K, MENEZES A. Analyzing the Galbraith-Lin-Scott point multiplication method for elliptic curves over binary fields [J]. IEEE

Transactions on Computers, 2009, 58(10):1411-1420.
[40] 国家商用密码管理办公室. http://www. oscca. gov. cn/
[41] POHLIG S, HELLMAN M. An improved algorithm for computing logarithms over GF(p) and its cryptographic significance[J]. IEEE TT, 1978, 24(1):106-110.
[42] SEMAEV I A. Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p[J]. Math Comp, 1998, 67(221):353-356.
[43] SMART N P. The discrete logarithm problem on elliptic curves of trace one[J]. Journal of Cryptology, 1999, 12(3):193-196.
[44] SATOH T, ARAKI K. Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves[J]. Comm Math Pauli, 1998, 47(1):81-92.
[45] MENEZES A, OKAMOTO T, VANSTONE S. Reducing elliptic curve logarithms to logarithms in a finite field [J]. IEEE Transactions on Information Theory, 1993, 39(2):1639-1646.
[46] FREY G, RÜCK H. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves[J]. Mathematics of Computation, 1994, 62: 865-874.
[47] GAUDRY P, HESS F, SMART N P. Constructive and destructive facets of Weil descent on elliptic curves[J]. Journal of Cryptology, 2002, 15(1):19-46.
[48] CLAUS D. The GHS attack in odd characteristic[J]. Journal of the Ramanujan Mathematical Society, 2003, 18(1):1-32.
[49] LAUTER K E, STANGE K E. The elliptic curve discrete logarithm problem and equivalent hard problems for elliptic divisibility sequences[M]//Roberto Maria Avanzi, Liam Kelleher, Francesco Sica. Selected Areas in Cryptography. Heidelberg: Springer-Verlag Berlin, 2009, 5381:309-327.
[50] POLLARD J. Monte Carlo methods for index computation mod p [J]. Mathematics of Computation, 1978, 32:918-924.
[51] VAN OORSCHOT P, WIENER M. Parallel collision search with cryptanalytic applications [J]. Journal of Cryptology, 1999, 12(1):1-28.
[52] CERTICOM. Certicom ECC challenge [EB/OL]. [2013-02-01]. http://www. certicom. com/images/pdfs/cert eccchallenge.
[53] BAILEY D V, BATINA L, BERNSTEIN D J, et al. Breaking ECC2K-130[R]. Cryptology ePrint Archive: Report 2009/541, 2009.
[54] BOS J W, KAIHARA M E, KLEINJUNG T. Solving a 112-bit prime elliptic curve discrete logarithm problem on game consoles using sloppy reduction [J]. International Journal of Applied Cryptography, 2012, 2(3):212-228.
[55] CHEON J H. Discrete logarithm problems with auxiliary inputs [J]. Cryptology, 2010, 23(3):457-476.
[56] ZHANG Fangguo, WANG Ping. Speeding up elliptic curve discrete logarithm computations with point halving [J]. Designs, Codes and Cryptography, 2013, 67(2): 197-208.
[57] SILVERMAN H, SUZUKI J. Elliptic curve discrete logarithms and the index calculus[C]//Proceedings of ASIACRYPT'98. Berlin: Springer-Verlag, 1998:110-125.
[58] JACOBSON M, KOBLITZ N, SILVERMAN J H. Analysis of the Xedni calculus attack [J]. Design, Codes, and Cryptography, 2000, 20(1):41-64.
[59] SEMAEV I. Summation polynomials and the discrete logarithm problem on elliptic curves[EB/OL]. [2013-01-26]. http://eprint. iacr. org/2004/031. pdf.
[60] PIERRICK G. Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem [J]. Journal of Symbolic Computation, 2008, 44(12):1690-1702.
[61] DIEM C. On the discrete logarithm problem in elliptic curves [J]. Compos Math, 2011, 147(1):75-104.
[62] JOUX A, VITSE V. Cover and decomposition index calculus on elliptic curves made practical [C]//Proceedings of EUROCRYPT. Berlin-Heidelberg: Springer-Verlag, 2012, 7237:9-26.
[63] FAUGÈRE J C, PERRET L, PETIT C, et al. Improving the complexity of index calculus algorithms in elliptic curves over binary fields [C]//Proceedings of EUROCRYPT. Berlin-Heidelberg: Springer-Verlag, 2012, 7237:27-44.
[64] CHENG Qi. Hard problems of algebraic geometry codes [J]. IEEE Transactions on IT, 2008, 54(1):402-406.
[65] MAURER U M. Towards the equivalence of breaking the Diffie-Hellman protocol and computing discrete logarithms[C]//Proceedings of the 14th Annual International Cryptology Conference on Advances in Cryptology. London:Springer-Verlag, 1994, 839:271-281.
[66] MUZEREAU A, SMART N P, VRECAUTEREN F. The equivalence between the DHP and DLP for elliptic curves used in practical applications[J]. LMS Journal of Computation and Mathematics, 2004, 7:50-72.
[67] SAKAI R, OHGISHI K, KASAHARA M. Cryptosystems Based on Pairing[C]//Symposium on Cryptography and Information Security (SCIS). Okinawa, Japan, 2000:26-28.
[68] JOUX A. A one round protocol for tripartite Diffie-Hellman[C]//Proceedings of the 4th International Symposium on Algorithmic Number Theory. London: Springer-Verlag, 2000, 1838:385-393.

[69] BONEH D, FRANKLIN M. Identity based encryption from the Weil pairing[J]//SIAM Journal on Computing, 2003, 32(3):586-615.

[70] WATERS B. Efficient identity-based encryption without random oracles[C]//Proceedings of EUROCRYPT. Berlin-Heidelberg: Springer-Verlag, 2005:114-127.

[71] SAHA I A, WATERS B. Fuzzy identity-based encryption//Proceedings of EUROCRYPT. Berlin-Heidelberg: Springer-Verlag, 2005, 3494:457-473.

[72] KATZ J, SAHAI A, WATERS B. Predicate encryption supporting disjunctions, polynomial equations, and inner products[C]//Proceedings of EUROCRYPT. Berlin-Heidelberg: Springer-Verlag, 2008:146-162.

[73] BONEH D, HAMBURG M. Generalized identity based and broadcast encryption schemes[C]//Proceedings of the 14th International Conference on the Theory and Application of Cryptology and Information Security. Berlin-Heidelberg: Springer-Verlag, 2008:455-470.

[74] BONEH D, LYNN B, SHACHAM H. Short signatures from the Weil pairing[C]//Proceedings of Asciacrypt'2001. New York: Springer-Verlag, 2001, 2248:514-532.

[75] ICART T. How to hash into elliptic curves[C]//Proceedings of CRYPTO. New York: Springer, 2009, 5677:303-316.

[76] ZHANG Fangguo, SAFAVI-NAIN I R, SUSILO W. An efficient signature scheme from bilinear pairings and its applications[C]//Proceedings of Public Key Cryptography PKC. New York: Springer-Verlag, 2004, 2947:277-290.

[77] BONEH D, BOYEN X. Short signatures without random oracles[C]//Proceedings of EUROCRYPT. Berlin-Heidelberg:Springer-Verlag, 2004, 3027:56-73.

[78] ZHANG Fangguo, CHEN Xiaofeng, SUSILO W, et al. A new signature scheme without random oracles from bilinear pairings[C]//Proceedings of VietCrypt'06. Berlin-Heidelberg: Springer-Verlag, 2006, 4341:67-80.

[79] ZHANG Fangguo. The computational square-root exponent problem-revisited[J]. Cryptology ePrint Archive, 2011:263.

[80] ROH D, HAHN S G. The square root Diffie-Hellman problem[J]. Designs, Codes and Cryptography, 2012, 62(2):179-187.

[81] MILLER V S. Short programs for functions on curves. Unpublished manuscript, 1986.

[82] DUURSMA I M, LEE H S. Tate pairing implementation for hyperelliptic curves $y^2 = x^p - x + d$[C]//Proceedings of ASIACRYPT. Berlin-Heidelberg: Springer-Verlag, 2003, 894:111-123.

[83] HESS F, SMART N P, VERCAUTEREN F. The Eta pairing revisited[C]//IEEE Transactions on IT, 2006, 52:4595-4602.

[84] ZHAO Changan, ZHANG Fangguo, HUANG Jiwu. A note on the Ate pairing[J]. International Journal of Information Security, 2008, 7(6):379-382.

[85] LEE E, PARK H L. Efficient and generalized pairing computation on Abelian varieties[J]. IEEE Transactions on IT, 2009, 55(4):1793-1803.

[86] VERCAUTEREN F. Optimal pairings[J]. IEEE Transactions on IT, 2010, 56(1):455-461.

[87] DEVEGILI A J, SCOTT M, DAHAB R. Implementing cryptographic pairings over barreto-naehrig curves[C]//Proceedings of the 1st International Conference on Pairing-Based Cryptography Pairing. Berlin-Heidelberg: Springer-Verlag, 2007, 4575:197-207.

[88] GRABHER P, GROβSCHÄDL J, PAGE D. On software parallel implementation of cryptographic pairings[M]//Roberto Maria Avanti, Liam Keliher, Francesco Sica. Selected Areas in Cryptography. Berlin-Heidelberg: Springer-Verlag, 2009, 5381:35-5.

[89] HANKERSON D, MENEZES A, SCOTT M. Identity-based cryptography[M]. Amsterdam: IOS Press, 2008, 12:188-206.

[90] NAEHRIG M, NIEDERHAGEN R, SCHWABE P. New software speed records for cryptographic pairings[C]//Proceedings of the 1st International Conference on Progress in Cryptology: Cryptology and Information Security in Latin America. Berlin-Heidelberg: Springer-Verlag, 2010, 6212:109-123.

[91] BEUCHAT J L, DÍAZ J E G, MITSUNARI S. et al. High-speed software implementation of the optimal Ate pairing over Barreto-Naehrig curves[C]//Proceedings of the 4th International Conference on Pairing-based Cryptography, Berlin-Heidelberg: Springer-Verlag, 2010, 6487:21-39.

[92] ARANHA D F, KARABINA K, LONGA P. Faster explicit formulas for computing pairings over ordinary curves[C]//Proceedings of EUROCRYPT. Berlin-Heidelberg: Springer-Verlag, 2011:48-68.

[93] GALBRAITH S D, HESS F, VERCAUTEREN F. Aspects of pairing inversion[J]. IEEE Transactions on Information Theory, 2008, 54(12):5719-5728.

[94] HAYASHI T, SHIMOYAMA T, SHINOHARA N. Breaking pairing-based cryptosystems using ηT pairing over $GF(3^{97})$[C]//Proceedings of the 18th International Conference on the Theory and Application of Cryptology and Information Security. Berlin-Heidelberg: Springer-Verlag, 2012, 7658:43-60.

[95] BROWN D R L, GJØSTEEN K. A security analysis of the NIST SP 800-90 elliptic curve random number generator[C]// Proceedings of the 27th Annual International

Cryptology Conference on Advances in Cryptology, 2007, 4622:466-481.

[96] GONG Guang, BERSON T A, STINSON D R. Elliptic curve pseudorandom sequence generators[C]//Proceedings of the 6th Annual International Workshop on Selected Areas in Cryptography. London: Springer-Verlag, 2000, 1999:34-48.

[97] BEELEN P, DOUMEN J. Pseudorandom sequences from elliptic curves[C]//Proceedings of 6th International Conference on Finite Fields with Applications to Coding Theory, Cryptography and Related Areas. [S. l.]: [s. n.], 2002:37-52.

[98] CHEON J H, CHEE S. Elliptic curves and resilient functions[C]//Proceedings of the 3rd International Conference on Information Security and Cryptology. London: Springer-Verlag, 2015:2000:64-72.

[99] BROWN D R L, ANTIPA A, CAMPAGNA M. et al. ECOH: the elliptic curve only Hash[R]. Certicom Corp First Round NIST SHA-3 Candidate, 2008.

[100] OMAR S, OUNI R, BOUANANI S. Hashing with elliptic curve L-functions[C]//Proceedings of the 4th International Conference on Arithmetic of Finite Fields. Berlin-Heidelberg: Springer-Verlag, 2012, 7369:196-207.

[101] GALBRAITH S D, HESS F, SMART N P. Extending the GHS Weil descent attack[C]//Proceedings of EUROCRYPT. Berlin-Heidelberg: Springer-Verlag, 2002, 2332:29-44.

[102] JAO D, MILLER S D, VENKATESAN R. Expander graphs based on GRH with an application to elliptic curve cryptography[J]. J Number Theory, 2009, 129(6):1491-1504.

[103] CHILDS A, JAO D, SOUKHAREV V. Constructing elliptic curve isogenies in quantum subexponential time [EB/OL]. [2013-01-25]. 2010. http://arxiv.org/abs/1012.4019/.

[104] FOUQUET M, MORAIN F. Isogeny volcanoes and the SEA algorithm[C]//Proceedings of the 5th International Symposium on Algorithmic Number Theory. London: Springer-Verlag, 2002: 276-291.

[105] DOCHE C, ICART T, KOHEL D. Efficient scalar multiplication by Isogeny decompositions [C]//Proceedings of PKC. Berlin-Heidelberg: Springer-Verlag, 2006, 3958:285-352.

[106] JAO D, MILLER S D, VENKATESAN R. Do all elliptic curves of the same order have the same difficulty of discrete log? [C]//Proceedings of ASIACRYPT 2005. Berlin-Heidelberg: Springer-Verlag, 2005, 3788: 21-40.

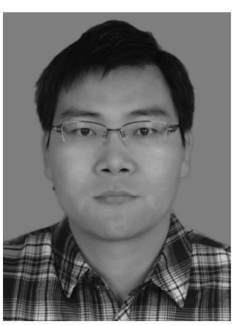
[107] CHARLES D, LAUTER K, GOREN AND E. Cryptographic hash functions from expander graphs[J]. Journal of Cryptology, 2009, 22:93-113.

[108] ROSTOVTSEV A, STOLBUNOV A. Public-key cryptosystem based on isogenies[R]. Cryptology ePrint Archive, 2006.

[109] STOLBUNOV A. Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves[J]. Adv Math Comm, 2010, 4(2):215-235.

[110] JAO D, DE FEO L. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies [C]//Proceedings of the 4th International Conference on Post-Quantum Cryptography. Berlin-Heidelberg: Springer-Verlag, 2011, 7071:19-34.

(编辑:许力琴)



张方国,中山大学信息科学与技术学院教授,博士生导师,广东省信息安全技术重点实验室副主任,中国密码学会常务理事。2001 年 12 月在西安电子科技大学获得工学博士学位。ProvSec2009,JWIS2011 和 AsiaJCIS 2012-13 的程序委员会主席,ICISC06-13, ASIACCS 11-13,中密会 09-13 等六十多个密码学与信息安全领域的国内外学术会议的程序委员会委员。研究兴趣为密码学理论及其应用,特别是:椭圆曲线和超椭圆曲线密码体制,安全多方计算,可证明安全,匿名性与隐私性等。