软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2016,27(3):760−767 [doi: 10.13328/j.cnki.jos.004922]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

公钥密码分析简介*

肖人毅

(国家自然科学基金委员会 信息科学部,北京 100085)

通讯作者: 肖人毅, E-mail: xiaory@nsfc.gov.cn

摘 要: 对公钥密码体制的密码分析历史的形成,给出一些重要结果的描述和重要文献的历史发展线索,同时对2010年~2014年有限域和椭圆曲线的离散对数问题的突破性进展给予了简单介绍.自公钥密码学1976年诞生以来,公钥密码体制的密码分析已经发展成为非常庞大的多学科交叉研究领域,希望可以给同行和学习密码学的研究生进入该领域起到帮助作用.

关键词: 公钥密码学;公钥密码分析;离散对数问题;信息安全

中图法分类号: TP309

中文引用格式: 肖人毅.公钥密码分析简介.软件学报,2016,27(3):760−767. http://www.jos.org.cn/1000-9825/4922.htm

英文引用格式: Xiao RY. Introduction to public key cryptanalysis. Ruan Jian Xue Bao/Journal of Software, 2016,27(3):760−767 (in Chinese). http://www.jos.org.cn/1000-9825/4922.htm

Introduction to Public Key Cryptanalysis

XIAO Ren-Yi

(Department of Information Sciences, National Natural Science Foundation of China, Beijing 100085, China)

Abstract: In this paper the historic development of public-key cryptanalysis and important literature are surveyed. In particular the breakthroughs during 2010~2014 about the discrete logarithm problems for finite fields and elliptic curves are described. Since the birth of public key cryptography, public key cryptanalysis has been developed to be an inter discipline research with tools from mathematics, algorithmic science and experimental simulations. This survey intents to help the young researchers in Chinese cryptologic community to enter this active research field.

Key words: public key cryptography; public key cryptanalysis; discrete logarithm problems; information security

公钥密码学的思想起源于Diffie与Hellman[1],提出把密码体制的加密密钥(公钥)与解密密钥(私钥)分开处理,以提高多用户保密通信的效率.其中,加密密钥是公开的,解密密钥是每个用户自己保密的,这样,从公钥计算出私钥是困难的.在这篇论文中,Diffie和Hellman并没有一个数学手段去实现他们的思想,而是提出实现公钥密码体制用单向函数(one-way function),直观地说,就是函数$f(x)$从x很容易计算$f(x)$,但从$y=f(x)$很难计算x.在这篇论文中,他们也讨论了在不安全信道下建立密钥的方法,即现在称为Diffie-Hellman密钥交换(亦称Diffie-Hellman-Merkle key exchange)的内容.这个问题Merkle差不多同时也给出了解决方法[2].Merkle后来的博士论文导师即是Hellman.

1977年,文献[3]就报道了3位MIT的学者设计出了第1个公钥密码体制.1978年,Rivest,Shamir和Adleman发表了文献[4],提出用两个素数乘积的模同余类的幂运算来实现公钥密码体制.其中的关键单向函数是从两个素数算出其乘积是容易的,但是任给一定规模大的数(即使知道其是两个素数乘积),将其分解为素数因子乘积是困难的.RSA公钥密码体制是专利技术,1982年成立的RSA公司即以其为基础向IT工业界提供安全产

* 收稿时间: 2015-03-09; 修改时间: 2015-05-20; 采用时间: 2015-06-13; jos在线出版时间: 2015-11-12
CNKI网络优先出版: 2015-11-11 17:04:06, http://www.cnki.net/kcms/detail/11.2560.TP.20151111.1704.008.html

品,2006 年被美国 EMC 公司收购.

实际上,公钥密码学思想和 RSA 公钥密码体制及 Diffie-Hellman-Merkle 密钥交换(key exchange)的思想在 1970 年~1976 年由为英国政府通信总部(government communications headquaters,简称 GCHQ)工作的数学家 Ellis(1970 年提出公钥密码体制思想),Cocks(1973 年提出 RSA),Williamson(1974~1976 年提出 key exchange)等人得到.GCHQ 是英国国家安全通信机构,为其工作的数学家的工作是否公开是由政府决定的.这些文件直到 1997 年才可公开.1997 年 12 月 18 日,在一个公开演讲中,Cocks 公开了这段历史,这时,Ellis 已经去世 22 天了.

1 公钥密码体制的早期密码分析与计算数论的起源

从 RSA 公钥密码体制和密钥交换(key exchange)的构造,人们已经清楚两类单向函数:一类是数的素数因子分解,一类是有限域的离散对数.这直接刺激了这两个数学问题的算法学研究,即计算数论学科的来源(computational number theory).例如,我们可以在文献[5−7]中知道计算数论的风格.文献[6]文预印本 1984 年开始流传,刺激了 1985 年 Koblitz[8]和 Miller[9]分别独立地提出椭圆曲线公钥密码体制,椭圆曲线公钥密码体制没有专利.

一般而言,对阶为 n 的抽象循环群,计算其离散对数是 $O\left(\sqrt{n}\right)$ 困难的,并且这是最好的可能(victor shoup),Coppersmith[7]提出的算法说明:对特征 2 的有限域的离散对数问题,算法是 $O\left(n^{\frac{1}{3}}\right)$ 困难的.

一般而言,对大数分解和有限域离散对数问题最好的算法是数域筛法(number field sieve)和函数域筛法,例如,在 Crypto2010 上就报道了此方法对一个 RSA-768 模数的分解[10].我们同样建议参考关于 RSA 模数分解报道的网站:http://smartfacts.cr.yp.to/

按照 Diffie 的论文[13],我们在公钥密码学的早期历史中必须提到的是 Merkle-Helleman 基于背包(knapsacks)公钥密码体制[15]和 McEliece 的基于代数编码(Goppa 编码)的公钥密码体制[14].在基于代数编码的公钥密码体制中,困难的问题是把代数编码伪装成一般编码,其解码问题(decoding)已经被 Berlekamp,McEliece 和 Tilborg 证明是 NP-完全.Diffie 写道:因为基于代数编码的 McEliece 公钥密码体制的公钥要求几乎百万级别的比特,所以看来是永远不会实际使用的.McEliece 公钥密码体制仍然是公钥密码分析的一个很受到注意的课题,可参见 Minder 等人的工作[16].

Merkle-Hellman 的背包(knapsack)公钥密码体制是基于子集合问题(subset sum problem)的,这是 NP-完全的问题,但其中用了 super-increasing,在其提出 4 年以后的 1982 年,Shamir[17,18]就用当时刚提出的格(lattice)的 LLL(Lenstra-Lenstra-Lovasz)算法破解,这是以后格算法在密码分析中扮演重要角色的起源.LLL 算法[19]是有理系数多项式分解的多项式时间算法,LLL 算法后来成为基于格的密码分析基石.

多变量多项式公钥密码体制起源于 Matsomoto-Imai 在 Eurocrypt 1988 会议上提出的 Matsomoto-Imai 方案,其想法是,基于解一般多变量代数方程组(即使是 2 次的)是 NP-完全[22].后来,在该体制被法国密码分析学者 Patarin 破解并发展[23,24],Matsumoto-Imai 更早期(1983 年)的一个用单变量多项式的公钥密码体制很快就被 Delsarte-Desmedt-Odlyzko-Piret 在 Eurocrypt 1984 会议上破解[20,21].关于这个领域最新的一些成果,我们可以参见 Dubois 和 Ding 近年的论文.

在 Diffie 的上述公钥密码学综述中[13],他也提到了 1979 年 Shamir 和 Blakley 提出的秘密共享,这后来成为理论密码学的重要基础理论安全多方计算的基础.

从早期公钥密码体制的密码分析的历史发展可以看出:人们原来设想的基于 NP-hard(完全)问题做些变形设计的公钥密码体制实际上都不牢靠,而基于分解(factoring)这个目前并不知道是不是 NP-hard 问题的 RSA 公钥密码体制反而经受住了考验.

公钥密码学早期的重要思想家包括:

- Whitfield Diffie(1944−),2010 年被授予 IEEE Richard W. Hamming 奖;

- Mrtin Hellman(1945−),2010 年被授予 IEEE Richard W. Hamming 奖,1987 年后投身于反战运动,从事原子战争的风险分析;
- Ralph Merkle(1952−),对公钥密码学的早期起源和密码 Hash 函数都做出贡献,2010 年被授予 IEEE Richard W. Hamming 奖,现在从事纳米技术研究;
- Rivest-Shamir-Adleman,2003 年被授予 ACM Turing award,这也是计算机科学界最高奖第 1 次授予密码学.第 2 次是 2012 年授予 ShafiGoldwasser(1958−)和 Silvio Micali(1954/10/13−);
- Ron Rivest(1947−),现在 MIT 工作.除 RSA 外,对密码 Hash 函数、电子选举都做出贡献;
- Adi Shamir(1952−),现在 Weizmann Institute of Science 工作.除 RSA,对于密码分析、秘密共享等做出多种贡献;
- Leonard Adleman(1945−),现在南加州大学,除 RSA 对计算数论的起源做出很大贡献,也是 DNA 计算的提出者.

2 有限域离散对数的 Barbulescu-Gaudry-Joux-Thome 算法

目前,关于有限域离散对数问题的最新进展见文献[11,12].前面提到的 Coppersmith 算法的思想对于有限域的离散对数问题的后续工作是重要的,Joux 于 2013 年在国际密码学会网站张贴的论文《A new index calculus algorithm with complexity $L(1/4+o(1))$ in small characteristic》首次提出经验式算法可以把小特征例如 2 的有限域离散对数算法计算量做到 $L(1/4)$,这个经验式算法依赖于一些有限域上多项式的假设.这个工作后来被他和合作者一起深化,即文献[11]的 Barbulescu-Gaudry-Joux-Thome(BGJT)算法,当然仍是经验式的.后来一些工作,如文献[12]等探讨了其经验式假设成立的情况及算法的修正,我们下面简单介绍 BGJT 算法的思路.

BGJT 算法的第 1 步是嵌入,这个思路是 Joux 的,就是把一个小特征的有限域 F_{p^n} 嵌入在 $F_{q^{2m}}$ 中,并且希望可以找到 F_{q^2} 上的低度数多项式 $h_0(x)$和 $h_1(x)$,使得 $h(x)=h_0(x)x^q-h_1(x)$有一个度数不超过 m 的不可约化因子多项式 $g(x)$可以表达有限域 $F_{q^{2m}}$.这一步需要经验式假设的.

BGJT 算法的第 2 步是用 $F_{q^2}[x]$ 中的首一线性多项式 $h(x)$, $F_{q^2}^*$ 的一个生成元作为指标计算法(index calculus)的分解基(factor base),并且要求出其所有关系.上面这些多项式都是模 $g(x)$运算的.由有限域的结果知道:上面的分解基确实是生成所有 $F_{q^{2m}}$ 的非零元素乘法群的,但是确定所有关系需要经验式假设.

BGJT 算法的最后一步(decent step)是将 $F_{q^{2m}}=F_{q^2}[x]/g(x)$ 中的非零元素表示为分解基中元素的乘积,这里也需要经验式假设才可以在拟多项式时间完成.

BGJT 算法本质上依赖于上述特定的低度数多项式表达有限域中元素、分解基关系的有效确定和最后一步的有效表达,其主要思想正如 Joux 在他 2013 年的论文提到的,是 Coppersmith 思想的非常广泛的拓展.目前,对这个算法的经验式假设在怎样情形成立有许多分析.在他们的论文里,对有限域 $F_{2^{4080}}$ 的离散对数进行了有效的计算.

3 RSA 密码分析的近期进展

3.1 经典结果

关于 RSA 的密码分析,1998 年,Boneh 的综述论文[25]仍然是很好的参考.近年来,德国学者 Alexander May 对 RSA 密码分析做了很多系统深入的工作,见 http://www.cits.rub.de/personen/may.html,这里只简单介绍以下几个方面.这些虽然不是实际使用 RSA 中最常见情况,但体现了目前的数学和算法学手段可以达到的高度.

(1) 小私钥情况

(2) 部分信息泄露情况

在情况(1),其典型的结果是 Wiener 于 1990 年的结果[26],如果模 $N=pq$,p 和 q 是满足 $q<p<2q$ 的素数,并且

私钥 $d<\frac{1}{3}N^{\frac{1}{4}}$,那么从公开的模 N 和公钥 e 可以多项式时间计算出私钥 d.这个结果在 1998 年被 Boneh 和 Durfee 改进为只要 $d<N^{0.292}$,也可以从模和公钥有效计算出私钥[27].

情况(2)的研究起源于 Coppersmith 在 1996 年提出的用 LLL 算法求整数系数的单变量多项式方程的小根[28],其应用于 RSA 密码分析有很多结果,例如,Coppersmith[28]当时给出:如果 RSA 模 N 是 n 比特的,如果 N 的某个素因子的最低或最高 $\frac{n}{4}$ 位置比特泄露,那么可以在多项式时间分解 N.这些研究在后来 May,Coron,Heninger,Shacham,Joux 等人的工作中有很多发展.

3.2 Heninger-Shacham经验式算法

实际使用 RSA 的密码分析常常是结合各种侧信道攻击(side-channel attack)得到部分信息加上情况 2)的数学和算法学的研究成果,见文献[29,30].

Heninger 和 Shacham 文献[30]的主要结果是:在小公钥 RSA 情况下,只要私钥 d 及 p,q,d_p,d_q 的 0.27 随机部分比特泄露,那么其给出的算法可以算出私钥.但是这个算法依然是经验式的,依赖于一些算法上的假设.

Heninger-Shacham 算法的主要数学思想来源于 Boneh-Durfee-Frenkle 于 1998 年在亚洲密码会的论文,在小公钥 e 的情况下,ed,ed_p,ed_q 关于$(p-1)(q-1),(p-1),(q-1)$的倍数是可以分析的,而其中实际的那个倍数是真实私钥对应倍数的很好逼近.这样,通过一系列算法实验找出真实的私钥 d,在模数 N 的因子 p 和 q 及私钥 d 的随机 0.42 部分比特泄露的情况下,他/她们的经验式算法也可以恢复私钥 d.

上述工作中的假设随机比特泄露比早期经典结果假设的特定比特泄露更接近实际情况,如文献[29]所提出的 cold boot 攻击下,实际是可能发生随机比特的泄露.

4 ECC 密码分析的最新进展

椭圆曲线公钥密码体制和 RSA 不同的是可以选择不同有限域上的不同椭圆曲线做出密码体制,很可能,这些不同的选择导致的公钥密码体制性质是完全不同的.我们主要叙述有限域上椭圆曲线上离散对数问题的研究进展,现状是可以区分出一些类别的椭圆曲线,其离散对数问题相比 $O(\sqrt{n})$ 困难的算法将更为有效.

4.1 经典结果

首先要提到的是 1993 年的基于 Weil pairing attack(MOV attack)[31],其基本原理是:可用 Weil pairing 将椭圆曲线的离散对数转化为一定扩域(指定义椭圆曲线基域的扩域)上的离散对数问题,在嵌入次数(embedding degree)不要太大,即,这个扩域不太大时,有限域的离散对数可以更有效解决.在文献[32]中,这个办法可以用椭圆曲线的 Tate pairing 实现.后来,一个本质的进步是 1998 年~1999 年的 Samaev[33],Satoh-Araki[35],Smart[34]这 3 人独立地区分出所谓的 Anomalous 椭圆曲线,即这种椭圆曲线对最低的基域 $GF(p)$,如果其 $GF(p)$有理点个数可被 p 整除,那么其离散对数也是可以有效求出的.

4.2 Gaudry-Hess-Smart攻击

Frey 在 1990 年代末期就提出,Weil decent(一种代数几何技巧)可以用来处理椭圆曲线的离散对数问题.Gaudry 等人对某些类别的超椭圆曲线的 Jacobian 得到一些关于 glog q 的有效算法后,结合这个想法,在 2000 年提出了基于 Weil decent 的离散对数算法,现在被广泛称为 Gaudry-Hess-Smart 攻击[36,37].其基本原理是:对复合基域,即,定义椭圆曲线的基域是 $GF(p^{mn})$形式,并且 Weil decent 转化为超椭圆曲线离散对数问题有效算法后,那么该椭圆曲线的离散对数问题存在有效算法.在文献[38,39]中,对一些具体的复合基域,Menezes 等人对其上有多少椭圆曲线可能对 GHS 攻击是虚弱的给出了分析.GHS 攻击后来还有发展,见 Smart 的网页http://www.cs.bris.ac.uk/~nigel/.

4.3 基于Samaev多项式的Gaudry-Diem攻击

Samaev 于 2004 年提出了关于有限域 F_{q^n} 上椭圆曲线的点和为 0 导致的坐标多项式关系[40],即:如果椭圆曲线上的点$(x_1,y_1),(x_2,y_2),\ldots,(x_m,y_m)$在椭圆曲线上和运算为 0,那么坐标点 $x_1,x_2,\ldots,x_m$ 必须满足多项式关系,这称为 m 阶 Samaev 和多项式,其算法时间是 $e^{m^2\log q}$ 的多项式.

Gaudry 和 Diem 提出了复合基域上的利用 Samaev 和多项式的指标计算(index calculus)算法,例如,Gaudry 的分解基(factor base)是 F_{q^n} 上椭圆曲线的使得其中坐标 x 在基域 F_q 中的所有点(x,y),而 Diem 的分解基是 F_{q^n} 上椭圆曲线的使得 x 在 F_{q^n} 的随机的 F_q 上线性子空间中的所有点(x,y),这时候,Samaev 和多项式就可以用来计算 F_{q^n} 上椭圆曲线上点的一系列表示为分解基的线性关系,这里实际上是表示为大量的代数关系式,所以 Gorbner 基方法也扮演了关键的角色.他们设计了算法,并理论上分析这将是很有效的[41,42].目前,这种算法的深入理解与实验分析是这个领域研究的重要热点,见文献[43,44].

5 补充及一些重要的密码分析学家

NTRU 是 1996 年 Brown 大学的数学家 Hoffstein,Pipher 和 Silverman 提出的公钥密码体制(包括数字签名),是利用整数系数多项式环的代数运算及模运算给出的密码体制.自提出以来,其安全性一直受到质疑.例如,Coppersmith 和 Shamir 给出了基于 LLL 恢复私钥的攻击[45].关于 NTRU 分析的近期进展,见文献[46−50].

关于格算法在公钥密码分析中的作用,见 Nguyen 的网页 http://www.di.ens.fr/~pnguyen/.

关于 Grobner 基算法在公钥密码分析中的作用,见 Faugere 的网页 http://www-salsa.lip6.fr/~jcf/.

重要的密码分析学家有:

- Adi Shamir,见第 2 节的描述;
- Don Coppersmith(1950−),重要的密码分析学者,对 RSA,NTRU 和有限域离散对数及数域筛法等做出重要贡献;
- Hendrik W. Lenstra(1949−),对整数分解算法(factoring)、LLL 算法、数域筛法等作出重要贡献;
- Arjen K. Lenstra(1956−),对整数分解算法(factoring)、LLL 算法、数域筛法、Hash 函数分析等做出重要贡献;
- Andrew Odlyzko(1949−),对有限域离散对数、背包(knapsack)密码体制分析、整数分解算法等做出重要贡献;
- Jacques Stern(1949−),法国密码学派的奠基人,在多变量公钥密码体制分析、格密码分析等领域起到开拓作用;
- Antoine Joux (1967−),对公钥密码体制的密码分析的各个领域做出重要贡献.

6 总结和展望

自公钥密码学诞生以来,随着公钥密码体制在通信和计算机网络中的大量使用,公钥密码体制的密码分析已经是一个国家国防、金融等关键部门信息安全保障实力的重要基础.此领域也已经发展成为大量使用计算机科学技术与数学的各种优秀成果达到密码分析目的多学科交叉研究领域.正是由于其交叉与需要大量算法实验等各种特点,在国内公开密码学界,集中从事公钥密码体制密码分析的研究人员还没有形成强大的研究队伍,本文可以给希望学习此研究领域的同行和研究生起到理清文献与历史发展线索的作用.

从 RSA 公钥密码体制的分析发展可以看出:May,Coron 等人的工作及第 3.2 节的 Heninger- Shacham 经验式算法以后,思路上没有突破,但是国际密码学界仍然非常重视 Coppersmith 利用格方法求整系数单变量方程小根的算法,并力图精化其思想,而且非常关注这个思想是不是可以拓展到多变量尤其是两个变量情况,这是一个值得关注的研究方向.

在最近几年,尤其是 2010 年~2014 年,在有限域离散对数和椭圆曲线离散对数问题上,国际密码学界与计算

数论界已经取得了突破性进展.国内密码学界和数学界开始关注这些领域的进展,如果年轻学者能够加强计算数论和算法学的基础学习,是可以迎头赶上的,对文献[11,12,29,30,41−44]中的经验式假设的分析进行更进一步的研究会很有益处.

公钥密码分析虽然经过多年的发展已经有大量文献,但是我们可以看出:其发展思路还是有线索可寻的,尤其是Coppersmith的一些思想,格算法和Gorbner基算法的巧妙使用都是极为重要的.学习这一领域的最新进展,并在这些工作基础上做出中国密码学者自己的世界水平的公钥密码分析工作,对国家的基本信息安全保障能力的真正提升做出贡献.

References:

[1] Diffie W, Hellman ME. New directions in cryptography. IEEE Trans. on Information Theory, 1976,22(6):644−654. [doi: 10.1109/TIT.1976.1055638]

[2] Merkle RC. Secure communications over insecure channels. Communications of the ACM, 1978,21(4):294−299. [doi: 10.1145/359460.359473]

[3] Gardner M. A new kind of cipher that would take millions of years to break. Scientific American, 1977,237:120−224. [doi: 10.1038/scientificamerican0877-120]

[4] Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 1978,21(2):120−126. [doi: 10.1145/359340.359342]

[5] Adleman LM. On distinguishing prime numbers from composite numbers. In: Proc. of the 21st Annual Symp. on Foundations of Computer Science. New York: IEEE, 1980. 387−406. [doi: 10.1109/SFCS.1980.28]

[6] Jr Lenstra HW. Factoring Integers with Elliptic Curves. Annals of Mathematics, 1987,126:649−673.

[7] Coppersmith D. Fast evaluation of logarithms in fields of characteristic two. IEEE Trans. on Information Theory, 1984,30(4):587−594. [doi: 10.1109/TIT.1984.1056941]

[8] Koblitz N. Elliptic curve cryptosystems. Mathematics of Computation, 1987,48(177):203−209. [doi: 10.1090/S0025-5718-1987-0866109-5]

[9] Miller VS. Use of elliptic curves in cryptography. In: Williams HC, ed. Proc. of the Advances in Cryptology—CRYPTO'85. Berlin, Heidelberg: Springer-Verlag, 1986. 417−426. [doi: 10.1007/3-540-39799-X_31]

[10] Kleinjung T, Aoki K, Franke J, Lenstra AK, Thome E, Bos JW, Gaudry P, Kruppa A, Montgomery PL, Osvik DA, te Riele H, Timofeev A, Zimmermann P. Factorization of a 768-bit RSA modulus. In: Rabin T, ed. Proc. of the Advances in Cryptology—CRYPTO 2010. Berlin, Heidelberg: Springer-Verlag, 2010. 333−350. [doi: 10.1007/978-3-642-14623-7_18]

[11] Barbulescu R, Gaudry P, Joux A, Thome E. A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. In: Nguyen PQ, Oswald E, eds. Proc. of the Advances in Cryptology—EUROCRYPT 2014. Berlin, Heidelberg: Springer-Verlag, 2014. 1−16. [doi: 10.1007/978-3-642-55220-5_1]

[12] Cheng Q, Wan D, Zhuang J. Traps to the BGJT-algorithm for discrete logarithms. LMS Journal of Computation and Mathematics, 2014,17(A):218−229. [doi: 10.1112/S1461157014000242]

[13] Diffie W. The first ten years of public-key cryptography. Proc. of the IEEE, 1988,76(5):560−577. [doi: 10.1109/5.4442]

[14] McEliece RJ. A public-key cryptosystem based on algebraic coding theory. DSN Progress Report, 1978,42(44):114−116.

[15] Merkle R, Hellman ME. Hiding information and signatures in trapdoor knapsacks. IEEE Trans. on Information Theory, 1978,24(5):525−530. [doi: 10.1109/TIT.1978.1055927]

[16] Minder L, Shokrollahi A. Cryptanalysis of the Sidelnikov cryptosystem. In: Naor M, ed. Proc. of the Advances in Cryptology—EUROCRYPT 2007. Berlin, Heidelberg: Springer-Verlag, 2007. 347−360. [doi: 10.1007/978-3-540-72540-4_20]

[17] Shamir A. A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem. In: Chaum D, Rivest RL, Sherman AT, eds. Proc. of the Advances in Cryptology. Springer-Verlag, 1983. 279−288. [doi: 10.1007/978-1-4757-0602-4_27]

[18] Shamir A. A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem. IEEE Trans. on Information Theory, 1984,30:699−704. [doi: 10.1109/TIT.1984.1056964]

[19] Lenstra AK, Lenstra HW, Lovász L. Factoring polynomials with rational coefficients. Mathematische Annalen, 1982,261(4):515−534. [doi: 10.1007/BF01457454]

[20] Matsumoto T, Imai H. A class of asymmetric crypto-systems based on polynomials over finite rings. In: Proc. of the IEEE Int'l Symp. on Information Theory. 1983. 131−132.

[21] Delsarte P, Desmedt Y, Odlyzko A, Piret P. Fast cryptanalysis of the Matsumoto-Imai public key scheme. In: Beth T, Cot N, Ingemarsson I, eds. Proc. of the Advances in Cryptology. Berlin, Heidelberg: Springer-Verlag, 1985. 142−149. [doi: 10.1007/3-540-39757-4_14]

[22] Matsumoto T, Imai H. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. In: Barstow W, ed. Proc. of the Advances in Cryptology—EUROCRYPT'88. Berlin, Heidelberg: Springer-Verlag, 1988. 419−453. [doi: 10.1007/3-540-45961-8_39]

[23] Patarin J. Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'88. In: Coppersmith D, ed. Proc. of the Advances in Cryptology—CRYPT0'95. Berlin, Heidelberg: Springer-Verlag, 1995. 248−261. [doi: 10.1007/3-540-44750-4_20]

[24] Patarin J. Asymmetric cryptography with a hidden monomial. In: Koblitz. N, ed. Proc. of the Advances in Cryptology—CRYPTO'96. Berlin, Heidelberg: Springer-Verlag, 1996. 45−60. [doi: 10.1007/3-540-68697-5_4]

[25] Boneh D. Twenty years of attacks on the RSA cryptosystem. Notices of the AMS, 1999,46(2):203−213.

[26] Wiener MJ. Cryptanalysis of short RSA secret exponents. IEEE Trans. on Information Theory, 1990,36(3):553−558. [doi: 10.1109/18.54902]

[27] Boneh D, Durfee G. Cryptanalysis of RSA with private key d less than $N^{0.292}$. IEEE Trans. on Information Theory, 2000,46(4):1339−1349. [doi: 10.1109/18.850673]

[28] Coppersmith D. Small solutions to polynomial equations, and low exponent RSA vulnerabilities. Journal of Cryptology, 1997,10(4):233−260. [doi: 10.1007/s001459900030]

[29] Halderman JA, Schoen SD, Heninger N, Clarkson W, Paul W, Calandrino JA, Felten EW. Lest we remember: Cold-boot attacks on encryption keys. Communications of the ACM, 2009,52(5):91−98. [doi: 10.1145/1506409.1506429]

[30] Heninger N, Shacham H. Reconstructing RSA private keys from random key bits. In: Halevi S, ed. Proc. of the Advances in Cryptology—CRYPTO 2009. Berlin, Heidelberg: Springer-Verlag, 2009. 1−17. [doi: 10.1007/978-3-642-03356-8_1]

[31] Menezes AJ, Okamoto T, Vanstone SA. Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Trans. on Information Theory, 1993,39(5):1639−1646. [doi: 10.1109/18.259647]

[32] Frey G, Rück HG. A remark concerning-divisibility and the discrete logarithm in the divisor class group of curves. Mathematics of computation, 1994,62(206):865−874. [doi: 10.2307/2153546]

[33] Semaev I. Evaluation of discrete logarithms in a group of P-torsion points of an elliptic curve in characteristic. Mathematics of Computation of the American Mathematical Society, 1998,67(221):353−356. [doi: 10.1090/S0025-5718-98-00887-4]

[34] Smart NP. The discrete logarithm problem on elliptic curves of trace one. Journal of Cryptology, 1999,12(3):193−196. [doi: 10.1007/s001459900052]

[35] Satoh T. Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves. Commentarii mathematici Universitatis Sancti Pauli, 1998,47(1):81−92.

[36] Gaudry P, Hess F, Smart NP. Constructive and destructive facets of Weil descent on elliptic curves. Journal of Cryptology, 2002, 15(1):19−46. [doi: 10.1007/s00145-001-0011-x]

[37] Hess F. Generalizing the GHS attack on the elliptic curve discrete logarithm problem. LMS Journal of Computation and Mathematics, 2004,7:167−192. [doi: 10.1112/S146115700000108X]

[38] Menezes A, Qu M. Analysis of the Weil descent attack of Gaudry, Hess and Smart. In: Naccache D, ed. Proc. of the Topics in Cryptology—CT-RSA 2001. Berlin, Heidelberg: Springer-Verlag, 2001. 308−318. [doi: 10.1007/3-540-45353-9_23]

[39] Menezes A, Teske E. Cryptographic implications of Hess' generalized GHS attack. Applicable Algebra in Engineering, Communication and Computing, 2006,16(6):439−460. [doi: 10.1007/s00200-005-0186-8]

[40] Semaev I. Summation polynomials and the discrete logarithm problem on elliptic curves. IACR Cryptology ePrint Archive, 2004, 2004:31.

[41] Gaudry P. Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem. Journal of Symbolic Computation, 2009,44(12):1690−1702. [doi: 10.1016/j.jsc.2008.08.005]

[42] Diem C. On the discrete logarithm problem in elliptic curves. Compositio Mathematica, 2011,147(1):75−104. [doi: 10.1112/S0010437X10005075]

[43] Faugère JC, Perret L, Petit C, Renault G. Improving the complexity of index calculus algorithms in elliptic curves over binary fields, In: Pointcheval D, Johansson T, eds. Proc. of the Advances in Cryptology—EUROCRYPT 2012. Berlin, Heidelberg: Springer-Verlag, 2012. 27−44. [doi: 10.1007/978-3-642-29011-4_4]

[44] Shantz M, Teske E. Solving the elliptic curve discrete logarithm problem using Semaev polynomials, Weil descent and Gröbner basis methods—An experimental study. In: Fischlin M, Katzenbeisser S, eds. Proc. of the Number Theory and Cryptography. Berlin, Heidelberg: Springer-Verlag, 2013. 94−107. [doi: 10.1007/978-3-642-42001-6_7]

[45] Coppersmith D, Shamir A. Lattice attacks on NTRU. In: Fumy W, ed. Proc. of the Advances in Cryptology—EUROCRYPT'97. Berlin, Heidelberg: Springer-Verlag, 1997. 52−61. [doi: 10.1007/3-540-69053-0_5]

[46] Howgrave-Graham N, Nguyen PQ, Pointcheval D, Proos J, Silverman JH, Singer A, Whyte W. The impact of decryption failures on the security of NTRU encryption. In: Boneh D, ed. Proc. of the Advances in Cryptology—CRYPTO 2003. Berlin, Heidelberg: Springer-Verlag, 2003. 226−246. [doi: 10.1007/978-3-540-45146-4_14]

[47] Gentry C, Szydlo M. Cryptanalysis of the revised NTRU signature scheme. In: Knudsen LR, ed. Proc. of the Advances in Cryptology—EUROCRYPT 2002. Berlin, Heidelberg: Springer-Verlag, 2002. 299−320. [doi: 10.1007/3-540-46035-7_20]

[48] Howgrave-Graham N. A hybrid lattice-reduction and meet-in-the-middle attack against NTRU. In: Menezes A, ed. Proc. of the Advances in Cryptology—CRYPTO 2007. Berlin, Heidelberg: Springer-Verlag, 2007. 150−169. [doi: 10.1007/978-3-540-74143-5_9]

[49] Stehlé D, Steinfeld R. Making NTRU as secure as worst-case problems over ideal lattices. In: Paterson KG, ed. Proc. of the Advances in Cryptology—EUROCRYPT 2011. Berlin, Heidelberg: Springer-Verlag, 2011. 27−47. [doi: 10.1007/978-3-642-20465-4_4]

[50] Perlner RA, Cooper DA. Quantum resistant public key cryptography: A survey. In: Proc. of the 8th Symp. on Identity and Trust on the Internet. New York: ACM Predd, 2009. 85−93. [doi: 10.1145/1527017.1527028]

肖人毅(1964－),男,北京人,博士,高级工程师,CCF 会员,主要研究领域为密码学,信息安全,计算机网络.