文章编号:1007－2985(2012)03－0027－05

椭圆曲线密码体制应用及脆弱性量子分析*

周学广
(海军工程大学信息安全系,湖北 武汉　430033)

摘　要:首先简要介绍椭圆曲线相关知识及其密码学应用,然后进行椭圆曲线加密体制(ECC)脆弱性分析,包括 ECC 的一般曲线分析、特殊曲线分析.重点提出了椭圆曲线上的离散对数脆弱性的量子分析方法.

关键词:椭圆曲线密码;公钥密码体制;离散对数;脆弱性分析;量子分析
中图分类号:TN918　　**文献标志码**:A　　**DOI**:10.3969/j.issn.1007－2985.2012.03.008

互联网的普及,使得网上电子数据交换需求激增.当前,适用于网络加密交换的主要技术是公钥密码体制,主要有 RSA 体制[1]、ElGamal 体制[2]和椭圆曲线加密体制(elliptic curve public-key cryptosystem,ECC).ECC 是 1985 年由 Neal Koblitz[3]和 Victor Miller[4]独立提出的,安全性建立在椭圆曲线离散对数的难解性上,同等密钥长度的条件下安全远高于 RSA 算法和其他算法,这也是 ECC 体制的重要优点.它意味着小的带宽和存储要求,因此,ECC 已成为主流的公钥密码体制,目前已有多个国际标准采用了 ECC.

由于量子计算机研发进展迅速,传统的公钥密码体制可能在未来某一天"突然失效",因此笔者提出用量子分析方法分析 ECC 的脆弱性.

1　椭圆曲线基本描述

1.1 椭圆曲线的定义

定义 1　设 F 是一个特征大于 3 的有限域,$a,b \in F$,则有限域 F 上的椭圆曲线 $y^2 = x^3 + ax + b$ 是由满足 F 上的方程 $y^2 = x^3 + ax + b$ 的所有点 $(x,y) \in F \times F$ 和另一个点 O(称为无穷远点)构成的集合 $E = \{O\} \cup \{(x,y) \in F \times F : y^2 = x^3 + ax + b\}$,有时也记为 $E(F)$,其中 $4a^3 + 27b^2 \neq 0$.

可以在 E 上定义一个加法群运算"+",其几何意义是:P 和 Q 是椭圆曲线上的 2 点,l 是连接 P 和 Q 的直线,若 $P=Q$,则 l 是 P 点的切线.R 是过 P 和 Q 的直线 l 与曲线的另一交点关于 x 轴的对称点.这样,$(E,+)$ 构成可交换群(Abel 群),O 是加法单位元(零元),如图 1,2 所示.

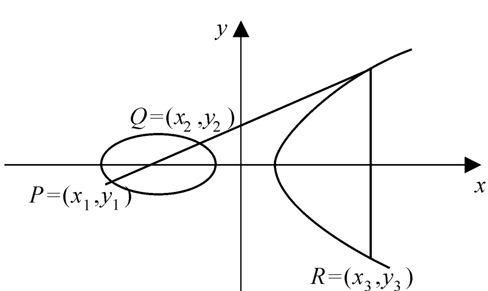

图 1　$P + Q = R$

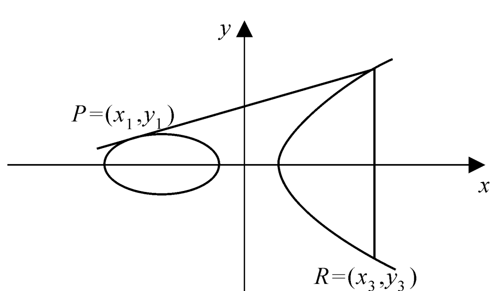

图 2　$P + P = 2P = R$

* 收稿日期:2012－01－13
作者简介:周学广(1966－),男,江苏高邮人,海军工程大学电子工程学院教授,博士,博士生导师,中国计算机学会(CCF)高级会员,主要从事密码学与信息安全研究.

定理 1 (1) $\forall P \in E$,定义 $P+O=O+P=P$;

(2) $\forall P=(x_1,y_1)\in E, Q=(x_2,y_2)\in E$,定义

$$P+Q=\begin{cases} O & 若\ x_1=x_2\ 且\ y_1=-y_2, \\ (x_3,y_3) & 其他, \end{cases}$$

其中 $\begin{cases} x_3=\lambda^3-x_1-x_2, \\ y_3=\lambda(x_1-x_3)-y_1, \end{cases}$ $\lambda=\begin{cases} \dfrac{y_3-y_1}{x_2-x_1} & 若\ P\neq Q, \\ \dfrac{3x_1^2+a}{2y_1} & 若\ P=Q. \end{cases}$

上述定义就是使 O 成为加法群 $(E,+)$ 的零元.

证明参见文献[5].

1.2 椭圆曲线群上的离散对数问题

定义 2 设 E 是有限域 F 上的椭圆曲线,$P\in E$,则 P 的阶 $\mathrm{ord}(P)$ 就是使 $nP=O$ 的最小的正整数,其中 O 是无穷远点,阶又称周期.

定义 3 设 E 是有限域 F 上的椭圆曲线,G 是 E 的一个循环子群,α 是 G 的一个生成元,即 $G=\{k\alpha: k\geqslant 1\}$,$\beta\in G$. 在已知 α,β 的条件下,求解整数 n,使得 $n\alpha=\beta$ 成立的问题,称为椭圆曲线 E 上的离散对数问题.

椭圆曲线 E 上的离散对数问题是困难问题,比有限域上的离散对数问题还难处理. 至今还没有出现类似于解有限域上离散对数问题的 index-calculus 算法来解一般椭圆曲线上的离散对数问题. 目前最好的一般方法的计算复杂性是 $0.88\sqrt{\mathrm{ord}(P)}$.

目前主要利用 Weil Pair 映射解决椭圆曲线离散对数问题,将有限域 $GF(q)$ 上椭圆曲线的离散对数问题转化为有限域 $GF(q^k)$ 上的离散对数问题,要求有限域 $GF(q)$ 应满足 $q>2^{160}$ 且 $q^k>2^{1\,024}$.

2 椭圆曲线密码体制的应用

椭圆曲线密码体制是基于椭圆曲线离散对数问题难解性的基础上的,其应用主要有加密/解密、数字签名等领域.

2.1 ECC 加密/解密

为方便椭圆曲线密码体制的计算,需要将明文嵌入作为椭圆曲线 E 上的一个点,也就是对明文信息的编码. 以 Menezes-Vanstone 公钥密码体制为例[6],具体描述如下:

设 E 是有限域 $F=GF(p)$ 上的椭圆曲线,p 为一个大素数,取 $\alpha\in E$ 是椭圆曲线上的一个点,且 $\mathrm{ord}(\alpha)$ 足够大,并使由 α 生成的循环群 $G=\{k\alpha: k\geqslant 1\}$ 中的离散对数问题是难解的. 公开 p,E,α.

随机选取整数 $d: 1\leqslant d\leqslant \mathrm{ord}(\alpha)-1$,计算 $\beta=d\alpha$,将其作为公开的加密密钥,将 d 作为保密的脱密密钥.

(1) 明文空间:$F^*\times F^*$,其中 $F^*=F\backslash\{0\}$.

(2) 密文空间:$E\times F^*\times F^*$.

(3) 加密变换:$\forall m=(m_1,m_2)\in F^*\times F^*$,秘密选择一个整数 $k(1\leqslant k\leqslant \mathrm{ord}(\alpha)-2)$,则密文为 $c=(c_0,c_1,c_2)$,其中 $c_0=k\alpha$,$c_1=k_1m_1 \bmod p$,$c_2=k_2m_2 \bmod p$,这里 $(k_1,k_2)=k\beta$.

(4) 脱密变换:$\forall c=(c_0,c_1,c_2)\in E\times F^*\times F^*$,明文为 $m=(c_1k_1^{-1} \bmod p, c_2k_2^{-1} \bmod p)$,其中 $(k_1,k_2)=dc_0$. 脱密变换能正确地从密文恢复相应的明文,证明参见文献[6].

2.2 基于椭圆曲线的数字签名

以美国批准的椭圆曲线数字签名算法(ECDSA)(FIPS186-2)为例.

设 p 是一个大素数或是 2 的幂次方,E 是定义在 F_p 上的椭圆曲线. 设 P 是椭圆曲线 E 上的一个阶为 q 的点,选取一个秘密的密钥 x,其对应的公钥为 $Y=xP$,$H(\cdot)$ 是一个安全的杂凑函数,若要对消息 m 进行签名,则 (r,s) 即为对消息 m 的签名,其签名算法如下:

(ⅰ) 选取一个秘密的随机数 $k(1\leqslant k\leqslant q-1)$;

(ⅱ) 计算$\begin{cases} kP=(u,v), \\ r=u \mod q, \\ s=k^{-1}(H(m)+rx) \mod q. \end{cases}$

验证算法：

(ⅰ) 计算 $w=s^{-1} \mod q$.

(ⅱ) 计算 $u_1=H(m)w \mod q$.

(ⅲ) 计算 $u_2=rw \mod q$.

(ⅳ) 验证$(u,v) \lesseqgtr u_1P+u_2Y$ 是否成立，这里用符号“$\lesseqgtr$”判断该式是否成立. 若成立，则接受该签名，否则拒绝. 证明参见文献[5].

3 椭圆曲线脆弱性分析

脆弱性又称安全性，是所有密码体制的核心问题. ECC 是建立在求椭圆曲线离散对数困难基础之上的，它的安全性依赖于椭圆曲线离散对数问题(ECDLP) 的安全性. 对 ECC 的脆弱性分析也成为当前密码学研究的一个热点. 下面简要介绍一般曲线分析法、特殊曲线分析法和量子算法分析法，需要深入研究的人员可参阅文献[7－10].

3.1 一般曲线分析

(1) Shanks算法 (时间-存储算法). Shanks算法也称为大步小步法(Baby step Giant step)算法，它是1978年以前求解ECDLP最好的算法. 设阶为n，这一算法的时间复杂度为$O(\sqrt{n})$，空间复杂度也为$O(\sqrt{n})$. 该算法是对“穷举搜索法”在时间和空间上的折衷.

(2) 指标计算法. 指标计算法的基本思想是利用$\log_\alpha p_i (1 \leqslant i \leqslant b)$来计算$\log_\alpha \beta$，这里 $p=\{p_1,p_2,\cdots,p_b\}$ 是一个“小”素数集合. 计算步骤如下：

(ⅰ) 选取 $x(1 \leqslant x \leqslant p-2)$，有 $\alpha^x \equiv p_1^{a_1} p_2^{a_2} \cdots p_b^{a_b} \pmod p$，计算出$\log_\alpha p_i$.

(ⅱ) 再随机选取 $s(1 \leqslant s \leqslant p-2)$，有 $\beta\alpha^s \equiv p_1^{c_1} p_2^{c_2} \cdots p_b^{c_b} \pmod p$，计算

$$\log_\alpha \beta + s \equiv c_1 \log_\alpha p_1 + c_2 \log_\alpha p_2 + \cdots + c_b \log_\alpha p_b \pmod p. \tag{1}$$

(1) 式中只有$\log_\alpha \beta$ 未知，其他都是已知的，因此可以很容易求出$\log_\alpha \beta$.

指标计算法是一种概率算法，只要“小”素数集合 $p=\{p_1,p_2,\cdots,p_b\}$ 和随机数 s 选取恰当，就可以计算出$\log_\alpha \beta$.

(3) Pollard ρ 方法. 1978 年 Pollard 提出了一种概率求解的方法，其时间复杂度大约是 $O(\frac{\sqrt{\pi n}}{2})$，与 Shanks 的大步小步法相当，但空间复杂度仅为 $O(1)$. 后来又提出如何将 Pollard ρ 算法分为 r 个进程并行处理，则时间复杂约为 $O(\frac{\sqrt{\pi n}}{2r})$. Pollard ρ 算法是已知的对一般椭圆曲线离散对数最好的攻击方法，攻击者利用 Pollard ρ 算法开展硬件攻击和软件攻击.

3.2 特殊曲线分析

(1) MOV 分析.

Menezes，Okamoto 和 Vanstone 在 1991 年发表了将 ECDLP 归约到有限域上离散对数的有效解法，并且以这 3 名作者的名字的第一个字母命名，即 MOV 归约.

算法 1　MOV 归约算法

输入：椭圆曲线 E 上阶为 n 的点 P，另一个点 Q.

输出：一个整数 L，$0 \leqslant L \leqslant n-1$，使得 $Q=LP$.

(ⅰ) 确定 k，使得 $E(n)=E(F_q)$；

(ⅱ) 找 $R \in E[n]$，使得 $\alpha=e_n(P,R)$ 是 n 阶元素；

(ⅲ) 计算 $\beta=e_n(Q,R)$；

(ⅳ) 计算 β 关于 α 在 F_q 中的离散对数；

(ⅴ) 输出 L.

MOV证明了当E是超奇异椭圆曲线时,扩域次数$k\leqslant 6$.所谓超奇异椭圆曲线,就是F_q的特征标是p整除$q+1-E(F_q)$的曲线.由此可以说明,这类椭圆曲线是有亚指数时间分析的.但MOV方法并不能适用于所有的椭圆曲线.

(2) FR分析.

Frey,Muller和Ruck利用Tate对,类似于MOV分析给出了椭圆曲线离散对数的一个分析方法.在利用MOV分析时,首先要求找到k,使得$E[n]\in E(F_q^*)$.在FR分析中并不要求上述条件,仅要求$n\mid(q-1)$成立,所以FR分析一般要比MOV分析适用的范围广,并且FR分析效率也比MOV分析效率高.

(3) Smart方法.

q是素数,对定义在F_q上且$E(F_q)=q$的椭圆曲线E被称为"畸形"(Anomalous)曲线.Smart在1988年提出了一种能够在$O(\ln q)$时间内求解这类曲线的方法.Smart方法构造了$E(F_q)$到F_q的加法群的一个同构映射,使在多项式时间内可求解这类ECDLP.

3.3 椭圆曲线上的离散对数问题量子分析

Shor P W[11] 最早于1995年给出了离散对数量子算法分析方法.受其启发,这里给出椭圆曲线上的离散对数问题的量子分析算法.

(1) 初始条件.对于$A,B\in E$,设$B=mA$,$rA=O$,椭圆曲线E满足上述定义.令$f(x_1,x_2)=x_1B-x_2A$,有$f[(x_1+k),x_2+k_s]=f(x_1,x_2)$,这里$(k,km)$是$f(x_1,x_2)$的周期.已知$A,B$求$m$的问题称之为椭圆曲线上的离散对数问题,简称ECDLP问题,该问题被认为是经典难题.

(2) 量子理论基础.设存在酉变换$\boldsymbol{U}$和本征向量$|\boldsymbol{\xi}\rangle$,如果存在复数u,使得$\boldsymbol{U}\mid\boldsymbol{\xi}\rangle=u\mid\boldsymbol{\xi}\rangle$,$u$就称为$\boldsymbol{U}$对于本征向量$|\boldsymbol{\xi}\rangle$下的本征值.定义量子态

$$\boldsymbol{\xi}_k=\frac{1}{\sqrt{r}}\sum_{i=0}^{r-1}\exp(-\frac{2\pi iks}{r})\mid sA\rangle$$

为酉变换$\boldsymbol{U}_A$和$\boldsymbol{U}_B$共有的本征向量,相应的本征值分别为$\exp(\frac{2\pi ikx}{r})$和$\exp(\frac{2\pi ikmx}{r})$.$\boldsymbol{U}_f\mid\boldsymbol{\xi}_k\rangle=\exp(\frac{2\pi ikx}{r})\mid\boldsymbol{\xi}_k\rangle$,其中$\mid x\rangle\boldsymbol{U}_A\mid y\rangle=\mid x\rangle\mid Axy\rangle$,$\mid x\rangle\boldsymbol{U}_B\mid y\rangle=\mid x\rangle\mid Bxy\rangle$.

(3) ECDLP量子分析算法.

算法2 ECDLP量子分析算法

输入:椭圆曲线上的2个点A,B.

输出:令$B=mA$成立的周期m.

(ⅰ) 建立初始态$\mid 0\rangle\mid 0\rangle\mid 0\rangle=\sum_{k=0}^{r-1}\mid 0\rangle 0\rangle\boldsymbol{\xi}_k\rangle$;

(ⅱ) 初始化3个寄存器为$\mid 0\rangle\mid 0\rangle\mid 1\rangle$;

(ⅲ) 设$l=2\log_2 N$,对前2个比特执行量子傅立叶变换(QFT)得$\sum_{k=0}^{r-1}(\sum_{s=0}^{2^l-1}\mid x\rangle)(\sum_{y=0}^{2^l-1}\mid y\rangle)\mid\boldsymbol{\xi}_k\rangle$;

(ⅳ) 分别对前2个寄存器执行酉变换$\boldsymbol{U}_A$和$\boldsymbol{U}_B$,得

$$\sum_{k=0}^{r-1}(\sum_{s=0}^{2^l-1}\exp(\frac{2\pi ikx}{r})\mid x\rangle)(\sum_{y=0}^{2^l-1}\exp(\frac{2\pi ikmy}{r})\mid y\rangle)\mid\boldsymbol{\xi}_k\rangle;$$

(ⅴ) 分别对前2个寄存器执行量子反傅立叶变换(QFT^{-1}),得$(\frac{k}{r})$,$(\frac{km}{r})$;

(ⅵ) 利用连分式运算计算出$m\bmod(\frac{r}{\gcd(k,r)})$的值,作为结果输出.

求函数周期的问题是量子算法中最为重要的应用之一,QFT也是仅有的以指数速度优越于经典算法的工具.用量子分析ECDLP问题,正是充分利用了量子算法分析的特长.

4　结语

ECC 建立在椭圆曲线理论基础上,是一种安全性高、计算量小、存储消耗小、带宽要求低的非对称加密算法,该系统的安全性已经得到公认.用量子分析方法分析 ECC,对今后应用量子计算机破译 ECC 提供了前期技术储备.

参考文献:

[1] RIVEST R L,SHAMIR A,ADLEMAN L. A Method for Obtaining Digital Signatures and Public Key Cryptosystems [J]. Communications of the ACM,1978,21(2):120 - 126.

[2] ELGAMAL L. A Public Key Cryptosystem and a Signature Scheme Base on Discrete Logarithm [J]. IEEE Trans. Info. Theory,1985,31:469 - 472.

[3] KOBLITZ NEAL. Elliptic Curve Cryptosystems [J]. Mathematics of Computation,1987,48:203 - 209.

[4] MILLER V. Uses of Elliptic Curves in Cryptography [C]//Advances in Cryptology CRYPTO'85,Lecture Notes in Computer Science. Berling:Springer-Verlag,1986,218:417 - 426.

[5] 金晨辉,郑浩然,张少武,等. 密码学 [M]. 北京:高等教育出版社,2009.

[6] MENEZES A J,OKAMOTO T,VANSTONE S A. Reducing Elliptic Curve Logarithms to a Finite Field [J]. IEEE Trans. Info. Theory,1993,9:1 639 - 1 646.

[7] XU Guang-wu. Short Vectors,the GLV Method and Discrete Logarithms [J]. Journal of Lanzhou University:Natural Sciences,2009,45(1):73 - 77.

[8] 陈智华. 基于 DNA 计算自组装的 Diffie-Hellman 算法破译 [J]. 计算机学报,2008,31(12):2 116 - 2 122.

[9] 司光东,董庆宽,李艳平,等. 一种基于离散对数群签名方案的分析 [J]. 哈尔滨工程大学学报,2007,28(10):1 131 - 1 134.

[10] 吕　欣,冯登国. 密码体制的量子算法分析 [J]. 计算机科学,2005,32(2):166 - 168.

[11] SHOR PETER W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer [J]. SIAM J. on Computing,1997,26(5):1 484 - 1 509.

Quantum Analysis on Vulnerability of Elliptic Curve Cryptosystem

ZHOU Xue-guang

(College of Electronic Engineering,Naval Engineering University,Wuhan 430033,China)

Abstract:The article introduces elliptic curve public-key cryptosystem and its related knowledge. It also analyzes security of elliptic curve public-key cryptosystem,which includes general analysis,special analysis and quantum analysis for vulnerability.

Key words:elliptic curve cryptosystem;public-key cryptosystem;discrete logarithm;vulnerability analysis;quantum analysis

(责任编辑　向阳洁)