【理论与探索】

用分布式并行算法选取 $GF(P)$ 上椭圆曲线的基点*

刘丹丹[1],张金山[2]

(1.成都理工大学 信息管理学院,成都 610005;2.乐山师范学院 数学系,四川 乐山 614004)

摘要:介绍有限域上定义的椭圆曲线及点群运算规则,给出椭圆曲线点群的阶.就大素数域上安全椭圆曲线基点的选取算法作了讨论,采用分布式并行算法,进一步改进优化,并借助于 MIRACL 系统用标准 C 语言对它们成功实现.实际测试结果表明,该工作确实加快了安全椭圆曲线基点的选取.

关键词:椭圆曲线;并行算法;基点;实现

中图分类号:TN918.1 **文献标识码**:A **文章编号**:1006-0707(2008)03-0107-02

自 1976 年 Diffie-Hellman 发明公开密钥密码体制之后,大量的公开密钥密码体制被陆续提出来,所有这些体制的安全性都依赖于数学问题的难解性.几十年来,许多曾经提出的公开密钥密码体制已经被攻破(即被证明是基于一个比原先想象要容易的问题),也有很多被证明是不实用的.迄今,只有 3 类体制被证明是安全和有效的,这些体制根据它们所依据的数学问题,可分类为:整数因式分解体制(RSA 是已知的最好例子),离散对数体制(如 ELGamal 体制,DSA),以及椭圆曲线密码体制(如 ECC),从目前 ECC 的实现结果来看,基于大素数域的椭圆曲线密码用软件实现要比基于特征 2 的 ECC 实现要快的多.本研究将对大素数域的椭圆曲线密码体制 $GF(p)$ 上椭圆曲线的基点选取算法进行讨论.首先,介绍有限域上定义的椭圆曲线及点群运算规则,给出椭圆曲线点群的阶.其次,采用分布式并行算法,改进文献[4]中的基点选取算法,并借助于 MIRACL 系统利用标准 C 语言对它们成功实现.

1 椭圆曲线

1.1 椭圆曲线定义

设 F_p 是一特征值大于 3 的有限素数域,则在仿射坐标平面上,定义在域 F_p 上的椭圆曲线 $E(F_p)$ 由满足下列方程的所有解 $(x,y) \in F_p \times F_p$ 及一个附加的无穷远点 $O(0,1,0)$ 组成:

$$E: y^2 = x^3 + ax + b \bmod p$$

其中:$a,b \in F_p$;$4a^3 + 27b^2 \neq 0 \bmod p$.

1.2 椭圆曲线点群运算规则

让 $E(F_p)$ 表示有限域上椭圆曲线解的集合,以及一个无穷远点 $O(0,1,0)$.椭圆曲线上的二点加的群运算规则可以通过"正切与正弦"加法运算及这个无穷远点来定义[3].

集合 $E(F_p)$ 对应下面的加法规则,且对加法"+"形成一个 Abel 群:

1) $\theta + \theta = \theta$ (单位元素).

2) $P + \theta = P \ \forall P \in E(F_p)$.

3) $(x,y) + (x,-y) = \theta$, $\forall P = (x,y) \in E(F_p)$,即点 (x,y) 的逆元为 $-P = (x,-y) \in E(F_p)$.

4) 令 $p = (x_1,y_1)$, $Q = (x_2,y_2)$, $P + Q = (x_3,y_3)$,则 $x_3 = \alpha^2 - 2x_1$, $y_3 = \alpha(x_1 - x_3) - y_1$.

其中: $$\alpha = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1} & P = Q \end{cases}$$

1.3 椭圆曲线上点群的阶

$\#E(F_p)$ 表示椭圆曲线 E 上的点的数量,Hasse 定理[8]证明了有限域 F_p 上的椭圆曲线上点群的阶满足下列公式:

$$\#E(F_p) = q + 1 + t \mid t \mid = \sqrt{p}$$

在 $GF(p)$ 上安全椭圆曲线的选取算法中,计算椭圆曲线点的个数 $\#E(F_p)$ 是最关键的一步.具体算法可参考文献[4].

* **收稿日期**:2008-03-26

作者简介:高丹丹(1983—),女,四川广安人,硕士研究生,主要从事代数数论方面的研究.

2 并行算法选取椭圆曲线的基点

要构造基于离散对数的密码体制,就必须找出椭圆曲线加法群的大素数因子子群的一个生成元,即基点.为找基点,先找椭圆曲线上任意一个随机点.

2.1 算法介绍

把多个处理器分成2部分, $S_i(i = 1,\cdots,s)$ 找椭圆曲线上的点 P, $T_i(i = 1,\cdots,t)$ 判断 P 是否为椭圆曲线群的基点.

首先,设 s 个处理器,在每个处理器上,随机选一个点 $x_i,(i = 1,\cdots,s)$,判断 x_i 是否为椭圆曲线上的点,若是,通知其他的处理器不能选此点,并将点 $P = (x_i, y_i)$ 存到能被 s 个处理器访问的公共表中.若否,通知其他的处理器下次不能选此点,而重新随机选点 x_i .

其次,设 t 个处理器,每个处理器在公共表随机选一个点 P ,判断 P 是否为椭圆曲线群的基点,若是,输出点 P ,并结束程序,否则,在公共表中删掉点 P ,而重新选取随机点.

2.2 并行算法

设 $\#E(F_p) = n = hk, k$ 是椭圆曲线 E 的阶的大素因子(至少 160 bit),下面算法是寻找有限域 $GF(p)$ 上的给定椭圆曲线上的基点的方法:

输入一个素数 $p > 3$, $GF(p)$ 上椭圆曲线 E 的参数 a, b ;

输出 E 上阶为 k 的点 G .

1) 在每个处理器上,随机选取 $x, 0 \leqslant x < P$.

2) 令 $\alpha \leftarrow x^3 + ax + b \bmod p$.

3) 如果 $\alpha = 0$,将点 $(x,0)$ 存到公共表中,通知其他的处理器不能选此点.

4) 如果 $\alpha \neq 0$,利用模 p 的平方根方法求 α 的一个平方根或判断它不存在.

5) 如果4)中的结果没有平方根存在,通知其他的处理器不能选此点,并返回 1). 否则 4)求出一个整数 $\beta, 0 < \beta < p$,使得 $\beta^2 = \alpha \bmod p$.

6) 生成一个随机比特 μ ,令 $y \leftarrow (-1)^{\mu}\beta$.

7) 将点 $P = (x, y)$ 存到公共表中.

8) 每个处理器 T_i 在公共表中随机选一个点 P.

9) 令 $G \leftarrow hP$.

10) 如果 $G = 0$,在公共表中删掉点 P ,并返回 8).

11) 输出 G .

注: ① 已知 P ,如何求 hP ? 即加速标量乘.在 $E(F_p)$ 中,由于已知 P ,易求 $-P$,故可利用标准二进制表示来加速标量乘.具体算法参考文献[5-6].② 在10)中的 G 是否为0,只需验证 $G = (x, y)$ 是否满足椭圆曲线方程 $y^2 = x^3 + ax + b \bmod p$,如果不满足,则认为 $G = 0$.

3 结束语

在本研究中,我们讨论了大素数域上的安全椭圆曲线的基点的选取.并借助 MIRACL 系统利用标准 C 语言对它们成功实现.实际测试结果表明,该工作确实加快了安全椭圆曲线基点的选取.

整个 ECC 的实现相当复杂,也许还存在一些我们尚未发现的问题.此外,设计与改进计算点的倍数算法及更底层的大整数除法等仍是尚待解决的难题.

致谢:在此,衷心感谢我尊敬的导师魏贵民教授的悉心指导!

参考文献:

[1] Koblitz1 N. E11iptic curve cryptosystems Mathematics of Computation[M]. [S.1.]: [s.n.], 1987, 45(17): 203 - 2091.

[2] V S miller1 use of elliptic curves in cryptography [C]//advances in cryptology cryptop85 proceedings. [S.1.]: springer-verlag, 1986: 417 - 426.

[3] 卢忱,严立军,卞正中.有限素整数域椭圆曲线密码体制基于代数几何快速算法设计[J].计算机工程与应用,2002,16:63 - 65.

[4] 张方国,王常杰,王育民. $GF(p)$ 上安全椭圆曲线及其基点的选取[J].电子与信息学报,2002,24(3):377 - 381.

[5] 孙琦,张起帆,彭国华.Dickson 多项式 $ge(x,1)$ 公钥密码体制的新算法[J].四川大学学报,2002,39(1): 18 - 23.

[6] 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[M].北京:电子工业出版社,2002.

[7] 岳光来,杨耀忠,韩子臣,等.局域网分布式并行计算环境的建立及应用[J].计算机工程与应用,2002(4): 136 - 138.

[8] 裴定一,祝跃飞.算法数论[M].北京:科学出版社,2002.

[9] 李俊全.椭圆曲线公钥密码体制的设计与分析[D].北京:中国科学院数学与系统科学研究院,2001.