网络安全管理保护现象进行了研究, 提出了基于遗传算法的入侵检测模型构建, 希望能够增加企业的网络安全防护质量, 促进其经济建设发展。

参考文献：

[1]朱亮. 基于遗传算法的网络安全技术的研究[J]. 电脑编程技巧与维护，2020（12）：170-172.

[2]付培玉，伍军，张小飞. 基于边缘计算和稳态遗传算法的 AIoT 资源调度研究[J]. 湘潭大学学报（自然科学版）, 2020, 42（05）：71-83.

[3]郭武士, 易欣. 基于遗传算法的煤炭企业网络安全技术的研究[J]. 煤炭技术，2012，31（02）：109-110+114.

[4]Cao Y，Fan X，Guo Y，et al. Multi-objective optimization of injection-molded plastic parts using entropy weight，random forest，and genetic algorithm methods[J]. Journal of Polymer Engineering，2020，40（4）：360-371.

[5]林芳. 基于 GA-SVM 网络安全技术研究[J]. 科技通报，2012，28（04）：176-177.

[6]任美玉, 符建厂. 网络安全态势评估与预测关键技术研究[J]. 网络安全技术与应用，2015（11）：124-125.

[7]刘锦伟，谢雄刚，方井. 基于遗传算法-BP 神经网络的煤层注水效果分析[J]. 工矿自动化，2016，42（01）：48-51.

[8]Li J，Ren S，Guo C . Synthesis of Sparse Arrays Based On CIGA（Convex Improved Genetic Algorithm）[J]. Journal of Microwaves，Optoelectronics and Electromagnetic Applications，2020，19（4）：444-456.

[9]秦涛，鲁冬林，郑国杰，等.基于遗传算法的某火炮高低伺服系统 SMC 研究[J].中国设备工程，2021（1）：127-129.

[10]王文鹏，邹刚，张玎，等.基于自适应遗传算法的舰载机保障调度[J].兵工自动化，2021，40（1）：37-42.

[11]张卓, 丛洪莲, 蒋高明, 等.基于交互式遗传算法的 Polo 衫快速款式推荐系统[J].纺织学报，2021，42（1）：138-144.

基于蒙哥马利域的 ECC 算法的优化

◆陈曼

（山东大学 数学学院　山东　250013）

摘要：由于现代社会通讯技术的发展，使得消息的传递更加方便，但同时伴随着消息被窃听，泄露，篡改的危险。为了安全的传递消息，许多加密算法随即被提出。本文主要讨论基于离散对数问题的椭圆曲线加密方案，通过结合几何与代数的思想来讨论椭圆曲线的运算规律，提出基于蒙哥马利域设计运行椭圆曲线加密解密程序，其相对于一般数域程序结果大概快了 10 倍。

关键词：椭圆曲线；蒙哥马利算法；加密算法

1　引言

随着信息通讯技术在经济社会的快速发展以及人人利用因特网传递信息, 如何安全的传输消息是现代经济社会需要考虑的一个崭新的问题。自从 1967 年 Diffle 和 Hellman 提出公钥算法，众多的密码方案随后产生，其中在传输信息阶段中经常用的公钥密码方案有 RSA 公钥密码体制和 DSA 数字签名方案。但为了保证加密算法传输信息的保密性，RSA 算法的密钥长度应大于 1000bit。所以，在存储空间固定时，网上带宽受到限制的情况下，在现有加密方案下建立实用的公钥密码体制十分困难。

为了解决上述难题，Neal Koblitz 和 Victor Miller 两人在 1985 年分别独立地提出了椭圆曲线加密算法。椭圆曲线加密方案相比于 RSA 加密算法，它运用了较高深的数学知识——椭圆曲线离散对数问题, 这能够减少对密钥长度的要求, 即椭圆曲线安全传输消息允许使用较短长度的密钥。椭圆曲线密码由于使用更短长度的密钥, 具有更小存储容量，更慢带宽的优势，能够广泛应用在线上支付，手机智能卡，无线传递信息。经过几十年的发展，椭圆曲线加密算法被各大国际组织机构广泛的使用，许多国际组织如 ANSI、IEEE、ISO 将椭圆曲线标准化。到目前为止，椭圆曲线数字签名机制 ECDSA 已成为经济贸易传输信息的加密标准。因此，针对椭圆曲线密码研究有效的优化算法，具有重要的实际用处和发展前景。

2　椭圆曲线密码储备知识

2.1 基本概念

椭圆曲线离散对数（ECDLP）[1] :离散对数问题是寻找到 $z \in N^+$，$b \in N$，和一个素数 P 的原根 a，使得 $b = a^z \mod p(0 \le z \le p-1)$。椭圆曲线离散对数是阶为 n 的椭圆曲线方程，P 点在椭圆曲线上，能够找到在椭圆曲线上的 Q 点，$Q = KP, (0 \le K \le n)$.

椭圆曲线点乘[1]：椭圆曲线 E 上的 P 点，和正整数 x，可以得出:

$xP = P + P + P + \cdots + P$

称为点乘运算，或为标量积。

椭圆曲线的阶：F_q 上椭圆曲线 E 中的点数 $\#E(F_q)$.

椭圆曲线 p 点的阶：令 $nP = O$ 的最小整数 n。

2.2 椭圆曲线

设椭圆曲线 E 是如下方程

$$F(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6,$$

可以推出椭圆曲线是齐次方程，且满足

$$\left(\frac{\partial F}{\partial x}(P), \frac{\partial F}{\partial y}(P), \frac{\partial F}{\partial z}(P)\right) \neq (0,0,0),$$

因而椭圆曲线上的每一点都是光滑的。定义椭圆曲线为 E，椭圆曲线上的运算规律记为 $\oplus$，椭圆曲线的运算法则示意图如图 1：

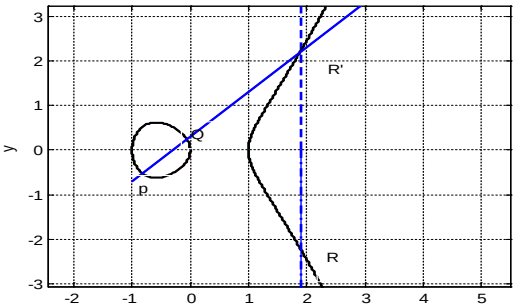

图 1 椭圆曲线运算法则

$(P \oplus Q) \oplus R' = O.$ 运算规律[2]：椭圆曲线 E 上的 P，Q 两点，L 是过 P，Q 两点（假如 $P = Q$，那么 L 是椭圆曲线上的切线），与椭圆曲线交于 R'，过 R' 做平行于 y 轴的直线，则与椭圆曲线 E 相交于

(C)1994-2021 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

点 R。

$(P \oplus Q = R)$因此椭圆曲线 E 上有如下的运算规律：

（1）椭圆曲线 E 上的直线 L 过 P,Q,R'，且 O 为无穷远点。

（2）$\forall P \subset E, P \oplus O = P.$

（3）$\forall P,Q \subset E, P \oplus Q = Q \oplus P.$

（4）设 $P \subset E$，存在椭圆曲线 E 上的一点 $-P$，则 $P \oplus -P = O.$

（5）$\forall P,Q,\ R \subset E, (P \oplus Q) \oplus R = P \oplus (Q + P),$

因而椭圆曲线 E 上的运算规律 $\oplus$ 构成了 $Abel$ 群。

例如特征域不为 2，3 上的椭圆曲线 $y^2 = x^3 + a_4 x + a_6$，$P_1(x_1, y_1), P_2(x_2, y_2)$是椭圆曲线上的两点，$O$ 为无穷远点，则椭圆曲线 E 的 $Abel$ 群的零元是无穷远点，逆元为 $-P_1 = (x_1, -y_1)$，并且 $P_3(x_3, y_3) = P_{1+}P_2 \neq O$。

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_x \\ y_3 = \lambda(x_1 - x_2) - y_1, \end{cases}$$

并且

$$\begin{cases} \lambda = \dfrac{y_2 - y_1}{x_2 - x_1}, (x_1 \neq x_2) \\ \lambda = \dfrac{3x_1 + a_4}{2y_1}, (x_1 = x_2) \end{cases}$$

2.4 椭圆曲线加密系统

通常将 F_p 上的椭圆曲线[3-4]描述为 $F(\mathrm{P}, a, b, p, n, h)$，其中 F_P 表示域，P 是极大素数。由于 P 越大，椭圆曲线加密算法复杂度越高，但降低了加密算法计算速度。a,b 两个未知数代表椭圆曲线方程，p 代表椭圆曲线上的基点，n 代表椭圆曲线上基点的阶，$h \leq 4$，其定义为：

$$h = \frac{\#E(F_q)}{order(n)}.$$

（1）例如 Alice 选择一条椭圆曲线 $E_{23}(1,1)$ $y^2 = x^3 + x + 1$，选择椭圆曲线 $E_{23}(1,1)$ 上 p（3.10）作为椭圆曲线上的基点，且基点的阶数是 28。

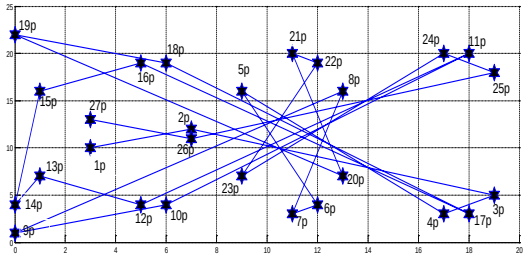

图 2 标乘 p 的值

其中 $-p = (3,13) = 27p$，则 $28p$=0，因此 p 的阶是 28。

（2）Alice 选择一个私钥 $k_A(1 \leq k_A \leq \mathrm{n})$，选择 $k_A = 18$，则 $K = k_A p = (6,19)$,Alice 将信息传递给 Bob，所传递的信息是 $E_{23}(1,1), K(6,19), p(3,10)$。

（3）Bob 接收到 Alice 传递过来的消息后，将 M 作为传输的信息，产生一个随机数 $r = 6, (r < n)$，要传输的信息是 11，因此 M 也应该在椭圆曲线上（11，3）：

$11^3 + 11 + 1 \equiv 3^2 (\mathrm{mod}\, 23).$

（4）Bob 需要计算

$C_1 = M + \mathrm{r}K = (11,3) + 6*18*p = (11,3) + 24p = (11,3) + (7,20) = (13,0),$

$C_2 = \mathrm{r}p = 6p = (12,4).$

（5）Bob 再将消息 C_1，C_2 传递给 Alice，因此 Alice 根据

$M = C_1 - k_A C_2 = M + rK - rk_A p = M + rK - rK,$

能够得到 M 的值。

3 基于蒙哥马利域上 ECC 算法的实现

椭圆曲线加密系统主要在于倍点运算。蒙哥马利算法[4]利用完全剩余系的性质，在计 ab(mod n) 时避免了 mod n 的除法运算，能够有效地提高模乘运算的速度。Montgomery 算法的基本思想是：计算 $\mathrm{abr}^{-1}(\mathrm{mod\ n})$；设 $2^{k-1} < n < 2^k$，$\mathrm{a} < n$，$\mathrm{b} < n$；$(n,r) = 1$，通常取 $\mathrm{r} = 2^k$；r^{-1} 是 r 模 n 的逆，即 $\mathrm{rr}^{-1} = 1(\mathrm{mod\ n})$；$\mathrm{rr}^{-1} - \mathrm{nn}' = 1$。因为 $\mathrm{r} = 2^k$，所以 mod r、/ r 都可以通过简单的移位操作实现，从而消去了最复杂的除法运算。

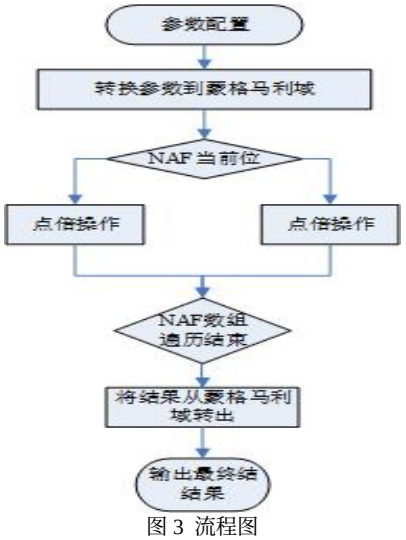

图 3 流程图

计算 $Mon\,Pro(a,b,r,n) = abr^{-1} \bmod n$

算法：

Step 1 $\mathrm{t} := a \cdot b$

Step 2 $\mathrm{u} := (t + (t \cdot n' \bmod r)n)/r$

Step 3 if $\mathrm{u} \geq n$ then

return $\mathrm{u} - n$

else return u

大数 bitmap 的实现：在 C 语言中，我们通过本来利用一般的思想的是一个数组位存一位数，存储 1024bit 的大数需要初始化数组 a[1024]，但是可以利用更节省空间的方法。C 语言 unsigned int 的范围是 $0 - 2^{32} - 1$，一个数组位就可以存 32bit（1 个 int = 4Byte.s = 4*8bit = 32 bit），1024 比特用初始化数组 a[1024 / 32] = a[33] 可以储存。 在本程序中，我用 a[0]代表实际数组的长度，因此 1024 比特位的大数需要用数组 a[33] 存储。

椭圆曲线参数的方程：$\mathrm{y}^2 = x^3 + 5$

q：

B640000002A3A6F1D603AB4FF58EC74521F2934B1A7AEEDBE56F9B27E351457D

椭圆曲线上的点 $p = (x, y)$

x：

93DE051D62BF718FF5ED0704487D01D6E1E4086909DC3280E8C4E4817C66DDDD

y：

21FE8DDA4F21E607631065125C395BBC1C1C00CBFA6024350C464CD70A3EA616

k：

02E65B0762D042F51F0D23542B13ED8CFA2E9A0E7206361E013A283905E31F

计算所得 $[k]p$。

比较直接用除法做 F_p 运算以及选择蒙哥马利域的运算结果（图 4、图 5）。

图 4 所用时间

(C)1994-2021 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

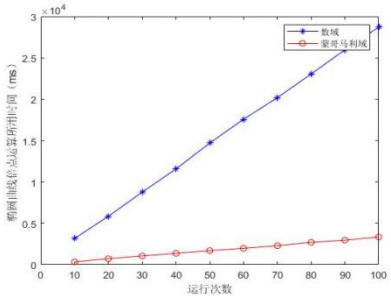

图 5 实验结果比较图

实验结果表明基于蒙哥马利域的椭圆曲线算法比一般数域下的速度快了 10 倍左右，其主要原因是一般除法太耗时间，而蒙哥马利算法通过位移就可以实现除法。

4 结束语

椭圆曲线是具有深厚历史，结合代数与几何知识的加密方案。本文简单介绍椭圆曲线的方程，运算性质，加密算法以及数字签名。本文利用数组 bitmap 思想实现大数存储，实现基于蒙哥马利域下的椭圆曲线算法。

参考文献：

[1]张方国.椭圆曲线在密码中的应用：过去，现在，将来…[J].山东大学学报（理学版），2013，48（05）：1-3.

[2]陈恭亮.信息安全数学基础[M].北京：清华大学出版社，2004：109-204.

[3]Andres.Elliptic curves and their application to crytography.Germany：University Augsburg，2001：11.

[4]贺令亚.蒙哥马利算法在 RSA 中的应用研究[J].现代计算机（专业版），2014（29）：7-9.

中文情感分析研究

◆闫婷婷　王恒[通讯作者]

（宁夏大学信息工程学院　宁夏　750000）

摘要：情感分析作为自然语言处理领域比较热门的研究方向，备受研究人员的关注。本文从情感分析的任务出发，对情感分类、情感信息抽取、情感信息的检索与归纳三个任务进行了介绍，重点阐述了情感分类研究中基于词典、基于机器学习的情感分类方法，最后本文介绍了情感分析的应用和情感分析的研究难点。

关键词：情感分析；情感分类；情感信息抽取；情感信息的检索与归纳

1 引言

随着互联网技术的快速发展，我国逐步向全面互联网时代迈进，根据 2020 年 4 月中国互联网络信息中心发布的第 45 次《中国互联网络发展状况统计报告》[1]显示，截至 2020 年 3 月，我国网民规模达 9.04 亿，互联网普及率达 64.5%。越来越多的人喜欢在微博、贴吧、论坛上对热点话题、国家政策、产品服务等内容进行交流讨论，发表个人意见、观点，表达情绪，从而产生了大量的主观性文本。对这些文本捕捉进行分析从而得到公众对事件或事物的看法，能够帮助政府部门获得相关舆情信息，消费者也能在购买产品时将获取相关评价内容作为参考依据。因此有效挖掘此类文本信息对舆情监控、电子商务、信息预测具有重要价值。文本情感分析成为目前学术界研究的一个热点。

2 情感分析研究内容

文本情感分析是指对用户表示的主观性文本进行分析和挖掘，是对网上各种新闻资讯、社会媒体和用户评论内容进行提取、分析、处理、归纳和推理的过程。根据处理文本粒度的不同，情感分析可分为词语级、短语级、句子级、篇章级等研究内容；根据情感分析研究的任务类型可分为情感信息提取、情感分类以及情感信息的检索和归纳等问题[2]。

2.1 情感分类

情感分类又称情感倾向性分析，主要用来判别文字中所表达的观点、喜好等相关信息。情感分类按照不同的划分方法导致划分结果也不同，可分为主、客观类，褒、贬类。按照分类粒度进行划分，可分为词语级、段落级和篇章级。本文主要从基于词典和语义规则的情感分类方法以及基于机器学习的情感分类方法进行说明。

2.2.1 基于词典和语义规则的情感分类方法

基于词典和语义规则的情感分类结合语法结构、设计的判别规则以情感词典作为判断情感倾向的主要依据。基于词典和语义规则的情感分类对文本进行情感分析的主要思路[3]是首先对文本进行预处理，使用标点符号进行分割，得到分句，经过设定好的情感词典、否定词典、程度副词词典，在不同的分句中，标注这些词出现的位置。按照不同的组合方式制定不同的权值计算方法。分析句间关系，通过对不同句型的处理强化情感分析的合理性，最终得到整体的情感分值，根据阈值来对文本分类。基于词典的情感分类关键在于词典的构建，目前国内外的情感词典的构建方法主要是在已有的情感词典的基础上扩充所需要的情感词典。顾宇杰在论文[4]中提到爬取微博评论数据进行过滤、分词、词性标注，其从微博评论数据中提取一部分词建立适合对明星微博评论进行情感分析的基础情感词典、程度副词词典和否定词词典，并设计了一套情感打分规则。从微博评论中选取 1000 条进行人工标注，使用词典和打分规则进行情感打分，通过计算正确率、召回率和 F-测度值来验证文中构建的情感词典以及打分规则的有效性。

2.2.2 基于机器学习的情感分类方法

基于机器学习的情感分类关键在于特征选择、特征权重量化以及分类模型等要素。常用的特征选择方法有信息增益法、基于文档频率的特征提取法、主成分分析法等。常用的特征量化方法有熵权重、布尔权重、TF-IDF 方法等。常用的分类器模型有朴素贝叶斯、支持向量机、K 近邻等。张柳等人[5]基于词云统计对文本内容进行特征分析，获取用户评论高频词，通过对高频词的降维高效训练朴素贝叶斯分类器，完成文本情感分类。最后展示出微博环境下的高校舆情情感演化图谱。

随着深度学习理论的不断发展，基于深度学习的算法被应用在各种领域，许多学者也将其用在文本处理中来试图提高文本分类的效果。深度学习是机器学习中发展的新领域。深度学习通过构建网络模型对文本分析、自动学习文本特征，优化模型输出来提高文本分类的准确性。秦欣在其论文[6]情感分析中对 N-Gram 切词生成的元组使用邻接熵和互信息进行边界自由度以及内部凝固度度量后得到的候选词集，使用词典过滤后得到新词集，将新词加入分词系统中来提高分

(C)1994-2021 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net