椭圆曲线密码体制安全性分析

李殿伟[1],王正义[2],赵俊阁[2]
(1. 海军司令部,北京 100841;
2. 海军工程大学 电子工程学院,湖北 武汉 430033)

摘 要: 椭圆曲线密码体制已成为当前最流行的公钥加密体制。为明确椭圆曲线密码的当前总体安全形势,首先研究椭圆曲线的定义及椭圆曲线离散对数问题,然后分别从安全椭圆曲线的选择方法、椭圆曲线密码的应用和针对椭圆曲线密码的攻击等几个方面,着重分析了椭圆曲线密码的安全性问题。根据与其它公钥密码体制的安全强度分析比较表明: 椭圆曲线密码体制具有许多优点,主要包括密钥短、安全强度高、加密快、运算量小、占用存储空间少等。因此椭圆曲线密码体制的研究具有重要的理论价值和广阔的应用前景。

关键词: 椭圆曲线密码; 公钥密码体制; 椭圆曲线离散对数; 安全性分析
中图分类号: TP309 **文献标识码**: A **文章编号**: 1673-629X(2012)04-0227-04

Analysis on Security of Elliptic Curve Cryptosystem

LI Dian-wei[1], WANG Zheng-yi[2], ZHAO Jun-ge[2]
(1. Office of Naval Headquarters, Beijing 100841, China;
2. College of Electronic Engineering, Naval Univ. of Engineering, Wuhan 430033, China)

Abstract: Elliptic curve cryptosystem has becoming the popular public-key cryptosystem gradually, thus it is important for us to comprehend its security state. Firstly, it has researched the definition of ECC and ECDLP. And then according to the selecting of elliptic curve as well as the application and the disverfied attacks of elliptic curve cryptosystem, the security analysis of elliptic curve cryptosystem was proposed in detail. Compared with other public-key cryptosystem, conclude that elliptic curve cryptosystem will be popularity in the future for the characters of short key, high security, fast encryption, little computation and small storage space. Therefore elliptic curve cryptosystem has important theoretical value and wide application prospect.

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

0 引 言

由于 Internet 网在全球范围内的迅速流行和普及,使得通过网络传输各种信息和数据的交换量迅猛增加,所以针对网络信息的安全问题日益凸显出来,从而对于各类信息的加密研究显得尤为重要。为了保证网络传输中各类信息的安全,现代通常使用的信息加密技术根据密钥类型不同可以划分为对称加密系统和非对称加密系统两大类。当前,普遍认为比较安全有效的公钥密码系统主要包括 RSA 体制、ElGamal 体制和椭圆曲线密码体制等。椭圆曲线密码体制(Elliptic Curve Cryptosystem,简称 ECC)是 1985 年由 Koblitz N[1] 和 Miller V[2] 提出的,其安全性是建立在求解椭圆曲线离散对数问题困难性基础上的,在同等密钥长度的情况下 ECC 体制的安全强度要远高于 RSA 体制等其它密码体制,因而 ECC 密码系统在网络信息安全领域有着非常重要的理论研究价值和广阔的实际应用前景[3]。另一方面,在安全性相当的情况下,ECC 体制所使用的密钥长度更短,这也就意味着对于带宽和存储空间的需求相对较小,并且到目前为止还没有出现针对于椭圆曲线的亚指数时间算法。因此,ECC 密码系统将会是今后最重要的主流公钥加密技术。

收稿日期: 2011-07-09; **修回日期**: 2011-10-15
基金项目: 全军军事学研究生课题(2010JY0700-404)
作者简介: 李殿伟(1965-),男,高级工程师,研究方向为装备技术与应用; 王正义(1988-),男,硕士研究生,研究方向为信息安全。

1 有限域上椭圆曲线的基本概述

1.1 椭圆曲线的几何意义

设 G 表示一个有限域,在其上定义一个椭圆曲线 E,实际上这个曲线 E 表示为一个点的集合,则有

$$E/G=\{(x,y)\mid y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6,\ a_1,\ a_3,\ a_2,\ a_4,\ a_6,x,\ y\in G\}\cup\{O\} \quad (1)$$

其中,O 表示无穷远点。

在椭圆曲线 E 上定义加法运算“+”,P 和 Q 是椭圆曲线 E 上的两个点,则对于这两个点的加法运算有 $P+$

$Q = R$。如图 1 所示，这里 R 表示为过点 P 和 Q 的直线与曲线 E 的交点关于 x 轴对称的椭圆曲线上的点。此时如果当 $P = Q$ 时，则 R 表示为 P 点的切线与曲线 E 的交点关于 x 轴对称的椭圆曲线上的点，如图 2 所示。这样，在有限域 G 上 $(E, +)$ 则构成了阿贝尔群，且其加法单位元为 O。

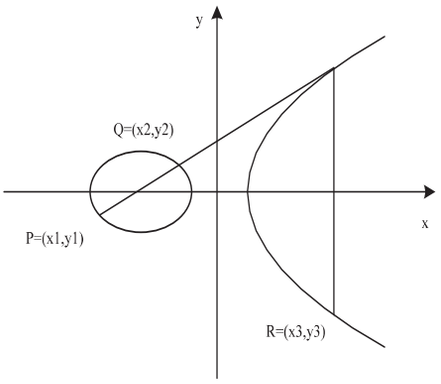

图 1 加法: $P + Q = R$

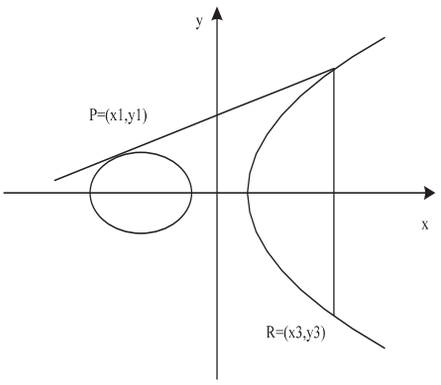

图 2 一点的 2 倍: $P + P = R$

设 $P = (x_1, y_1) \in E$，$Q = (x_2, y_2) \in E$，如果 $x_1 = x_2$ 且 $y_1 = -y_2$，那么则有 $P + Q = O$; 否则，加法运算 $P + Q = (x_3, y_3)$，这里的 $x_3 = \lambda^2 - x_1 - x_2$，$y_3 = \lambda(x_1 - x_3) - y_1$，其中

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1}, & P = Q \end{cases} \tag{2}$$

1.2 椭圆曲线上的离散对数问题

椭圆曲线离散对数问题(Elliptic Curve Discrete Logarithm Problem，简称 ECDLP)[4] 是指在有限域 F_q 上定义一条椭圆曲线 E，在其上给定一个基点 $P \in E(F_q)$，并计算出其阶 N，然后对于这条曲线 E 上的任意一点 Q，在 $[0, N-1]$ 范围内找到一个正整数 k，使得有 $Q = kP$ 成立，此时称正整数 k 为点 Q 对于点 P 的椭圆曲线离散对数，则有正整数 k 可以表示为:

$$k = \log_p Q \tag{3}$$

由于已知椭圆曲线离散对数 k 和基点 P 计算出点 Q 是比较容易的，然而由点 Q 和 P 计算出椭圆曲线离散对数 k 则是非常困难的，所以迄今为止仍然没有比较有效的方法来解决这个难题，正是由于这个原因在其基础上建立了椭圆曲线密码体制，这正是椭圆曲线密码的加密原理所在[5]。需要注意的是，由于椭圆曲线上的离散对数问题是比大整数的因子分解问题要难得多的数学难题，所以在此基础上建立的 ECC 密码体制在传统的数学攻击范畴内具有较高的安全性。

1.3 椭圆曲线的选择方法

在 ECC 体制中并不是全部的椭圆曲线都可以应用于公钥密码体制中，所以为了保证椭圆曲线密码能够抵抗各种数学攻击，必须选取椭圆曲线的阶是大素数或是含大素数因子的椭圆曲线。通常使用的安全椭圆曲线主要是由四种选择方法获得的，下面给出具体的选取方法。

方法一: 首先找到一个椭圆曲线的阶，其中这个阶必须满足安全椭圆曲线的阶的安全条件，即该阶必须是大素数或者含大素数因子的整数，然后根据这个符合安全条件的阶从而可以构造出一个所需要的安全椭圆曲线。

方法二: 首先在给定的有限域 F_q 上通过随机生成一个椭圆曲线，同时直接计算出这个椭圆曲线的阶，然后根据安全椭圆曲线的阶的安全条件判断这个曲线的阶是否为大素数或是含有大素数因子。如果是则该椭圆曲线即为所需要的安全曲线，否则继续重复上述步骤直至产生符合安全条件的椭圆曲线。

方法三: 首先选取具有一定特殊性的椭圆曲线系数，根据所选取的诸多系数确定一个椭圆曲线，同时依据所选择的参数计算出这个椭圆曲线的阶，然后根据安全椭圆曲线的阶的安全条件判断这个曲线的阶是否为大素数或是含有大素数因子。如果是则由所选取参数确定的椭圆曲线即为所需要的安全曲线，否则继续重新选择参数直至产生符合安全条件的椭圆曲线。

方法四: 首先对于一个给定的有限域 F_q，如果参数 q 满足条件 $q = 2^m$(其中，m 是一个能被较小整数 d 整除的正数)，那么在有限域 F_{q_1}(这里，$q_1 = 2d$) 上选择一个椭圆曲线 E'，同时直接计算出这个曲线 E' 在扩域 F_q 上的阶，假如这个曲线在扩域上的阶符合安全标准，则可以在此基础上找出椭圆曲线 E' 在有限域 F_q 上的嵌入椭圆曲线 E，此时所得到的椭圆曲线 E 即为所需要的安全椭圆曲线，否则重新选择椭圆曲线 E' 直至产生符合安全条件的椭圆曲线。

由于安全的椭圆曲线密码算法需要有好的安全椭圆曲线支撑，而对于一个好的安全椭圆曲线则是需要能够抵抗现有的各种攻击，因此选择一个好的椭圆曲线对于椭圆曲线密码体制显得尤为重要。目前，由上述四种方法所产生的比较流行的计算椭圆曲线的阶常

用算法主要包括复杂乘数算法、SEA 算法和 Satoh 算法等。

2　椭圆密码体制的应用

椭圆曲线密码体制是基于求解椭圆曲线中离散对数问题难解性基础之上的[6]，其目前应用范围主要有加密/解密、数字签名、身份认证等领域，下面将给出基于椭圆曲线密码的加解密和数字签名具体实现过程。

2.1　椭圆曲线密码的加解密过程

在利用椭圆曲线密码进行加密的过程中，为了方便实现每一步的计算，需要把明文消息 M 嵌入椭圆曲线 $E(a,b)$ 内作为其上的一个点，也就是说首先需要对明文消息 M 进行信息编码。如果当所发送的明文信息较长时，则可以通过将明文消息分段嵌入进行加密，具体反映在椭圆曲线密码中即是需要进行多标量乘法运算。

下面描述一个利用椭圆曲线密码实施加密通信的具体过程: 假设发送者 A 和接收者 B 之间需要进行加密传输通信，那么首先需要把所需发送的明文消息 M 编码为椭圆曲线 $E(a,b)$ 上的一个点 Q，此时则可以得到相关的椭圆曲线密码参数为 $T=(Q,a,b,P,N)$。

step1. 首先选择一个椭圆曲线 $Ep(a,b)$ 以及其上的一个基点 P，并计算出这个曲线的阶 N。此时发送者 A 在 $[1,N-1]$ 范围内随机选取一个正整数 k_A 作为私钥进行保存，然后根据公式 $Q_A=k_AP$ 产生 A 自己的公钥; 而接收者 B 同时也在 $[1,N-1]$ 范围内随机选取一个正整数 k_B 作为私钥进行保存，然后根据公式 $Q_B=k_BP$ 产生 B 自己的公钥。

step2. 发送者 A 选取一个随机的正整数 d，计算出密文消息 $C=\{dG,Q+dQ_B\}$ 发送给接收者 B，在这里发送者 A 计算密文消息时需要使用接收者 B 的公钥 Q_B。

step3. 接收者 B 收到密文$\{kP,C\}$ 后进行解密需要做如下运算:

$$Q+dQ_B-k_B(dP)=Q+d(k_BP)-k_B(dP)=Q+d(k_BP)-d(k_BP)=Q$$

对于目前已知的各种攻击算法而言，相对于 RSA 等其它公钥密码体制，椭圆曲线密码体制的计算量可以减少近 20 倍，所需的密钥长度同样可以减少大约 2 到 3 倍。因此椭圆曲线密码体制在安全性和计算实现等方面都要比 RSA 密码体制具有更大的优越性。

2.2　基于椭圆曲线密码的数字签名

定义一个椭圆曲线 $Ep(a,b)$ 和其上的基点 P，其中 N 是 P 的阶。Q 为曲线 $Ep(a,b)$ 上任意一点，令 $Q=kP$ 建立公私密钥对，其中 k 为私钥，Q 为公钥可以公开。

下面给出发送者 A 和接收者 B 之间利用椭圆曲线密码进行数字签名的具体过程[7]:

step1. 首先利用 Hash 函数对明文消息 M 进行计算，其中，常用的 Hash 函数算法有 MD5 算法或 SHA-1 算法，可以计算出明文消息 M 的摘要值 $t=H(M)$;

step2. 然后在区间 $[1,N-1]$ 范围内随机选取一个整数 k 作为此次签名的私钥;

step3. 计算出公钥 $Q=kP$;

step4. 计算 $r=Q_x \bmod N$，其中，Q_x 是表示公钥 Q 的横坐标，如果 $r=0$，则返回到 step2;

step5. 计算 $s=k^{-1}(t+rk) \bmod N$，其中 k 为发送者 A 的私钥，如果 $s=0$，则返回到 step2;

step6. 发送者 A 把消息签名(r,s) 传送给接收者 B。

接收者 B 收到消息签名(r,s) 后，对消息签名的具体验证过程如下:

step1. 首先对消息签名 r 和 s 进行验证，即判断其是否是在区间 $[1,N-1]$ 范围内的正整数，如果该签名不符合消息签名的条件，则认为收到的消息签名(r,s) 不是有效合法的签名;

step2. 根据所获得发送者 A 的签名公钥 Q_A，利用发送者 A 和接收者 B 具有相同的 Hash 函数摘要值，计算出待签名明文消息 M 的摘要值 $t=H(M)$;

step3. 计算出参数值 $e=s^{-1} \bmod N$;

step4. 计算出参数值 $u=te \bmod N$;

step5. 计算出参数值 $v=re \bmod N$;

step6. 计算出参数值 $R=uP+vQ$;

step7. 如果 $R=0$，则接收者 B 可以拒绝签名。否则，计算 $v=R_x \bmod N$，其中 R_x 是表示参数 R 的横坐标;

step8. 如果所计算的参数值 v 与 r 是相同的，则可以认为发送者 A 对明文消息 M 的签名被接收者 B 验证通过，即该签名是合法有效的。否则，该签名不是合法有效的，接收者 B 可以拒绝此签名。

基于椭圆曲线密码算法的数字签名方法，一方面是因为这种方案能够避免求阶运算中的模逆运算，因而比基于离散对数方案的签名算法要简单; 另一方面则是因为计算明文消息摘要 $H(M)$ 要比计算 $H(M,R)$ 简单，所以其运算速度要比 Schnorr 数字签名方案的运算速度快得多。因此，基于椭圆曲线密码的数字签名方案在抗攻击的安全强度、密钥长度、运算速度、计算代价与带宽要求等方面中具有很好的应用优势[8]。

3　椭圆曲线与其它密码体制的安全性比较

各种密码算法的安全性是所有密码体制最核心最关键的问题，同时也是从事密码研究工作的专业人士

最关心的方面。对于椭圆曲线密码体制来说，它的安全性是建立在求解椭圆曲线离散对数困难基础之上的，这也就是说椭圆曲线密码的安全性在很大程度上是依赖于椭圆曲线上的离散对数问题(ECDLP) 的求解困难性。然而由于椭圆曲线密码体制已经成为目前最流行的公钥密码体制之一，所以随之而来的各种针对 ECC 加密算法的攻击技术和防御技术逐渐成为当前密码学研究领域中的一个热点问题[9] 。当前针对一般椭圆曲线的攻击方法主要有: Shanks 算法、指标计算法、Pohlig-Hellman 算法和 Pollard ρ 算法等; 而针对一些特殊椭圆曲线的攻击方法主要有 MOV 攻击、FR 攻击和 Smart 方法等。

研究表明迄今为止仍然没有发现比较有效的计算 ECDLP 的方法，当前阶段能够找到的计算 ECDLP 最好的算法依然是指数时间内的并行 Pollard ρ 计算方法。需要注意的是从理论上证明 ECDLP 的求解不存在亚指数时间内的攻击方法已经是不可能的，所以寻找求解 ECDLP 的亚指数时间甚至多项式时间内的攻击算法具有非常重要的意义[10] ，目前，公钥密码体制的建立都是基于一个在数学计算上安全的数学难题，但是随着具有无限计算能力的新型计算机(例如量子计算机、DNA 计算机[11] 等) 的研究，基于各类数学难题的公钥密码体制将会变得越来越不安全，虽然这还需要经历一个较长的阶段，然而这将促使我们必须去寻找具有可证明安全性的新型密码。因此，对于 ECDLP 的在亚指数时间甚至多项式时间内的攻击算法的寻找将是今后较长时间内密码学领域安全性研究一项非常重要和必要的课题。

当前比较安全有效的公钥密码体制主要包括有 RSA 密码算法、DSA 密码算法和 ECC 密码算法等。其中，目前使用最广泛的公钥加密算法是 RSA 密码体制，它的安全性是建立在大整数素因子分解困难性基础之上的，但是由于随着大整数分解和计算机并行处理技术的快速发展，当前所采用的各类公钥密码体制中都必须要进一步增加密钥的长度，这样才能实现密码算法相对的安全性，然而这同时将使得密码算法的计算变得更加复杂、计算速度更慢。自从 1985 年关于椭圆曲线的理论被应用到密码学体系以来，在其基础之上建立起来的椭圆曲线密码体制已逐步成为迄今最流行的公钥密码体制，这一方面是由于椭圆曲线密码体制在安全性较好的条件下，可以使用长度更短的密钥，另一方面是由于椭圆曲线的资源非常丰富，在相同的一个有限域内存在大量不同的椭圆曲线，可以利用 1.3 节给出的方法选择好的安全椭圆曲线，这不仅为生成一个安全强度高的椭圆曲线密码体制增加了额外的安全保障，而且同时也为椭圆曲线密码算法在软硬件的实现等方面带来更大的方便。

对于 RSA 公钥密码体制来说，它的安全强度主要取决于其使用密钥的长度，然而伴随着计算机技术的飞速发展，512 位长度的密钥已不再安全，而 2048 位长度的密钥在未来一段时间内将会被认为是安全的。而椭圆曲线密码体制在加密强度相同的前提下，所需的密钥较短，下面给出 RSA/DSA 与 ECC 的安全性比较，具体比较结果如图 3 和表 1 所示[12] (其中，一般认为破译时间为 10^{12} MIPS 年表示该密码算法是安全的) 。

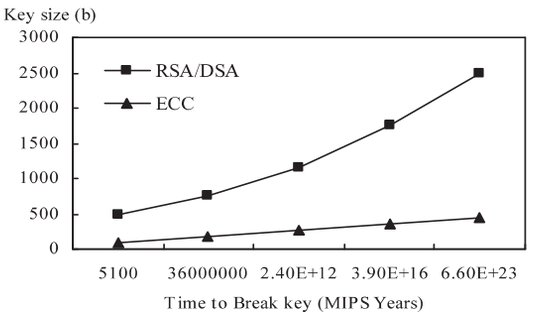

图 3 RSA/DSA 与 FCC 的安全性比较

表 1 RSA/DSA 和 ECC 的密钥长度比较结果

破解时间	RSA/DSA 密钥长度	ECC 密钥长度	密钥长度比
1.0×10^{4}	5.12×10^{2}	1.06×10^{2}	4.8:1
1.0×10^{8}	7.68×10^{2}	1.32×10^{2}	5.8:1
1.0×10^{12}	1.024×10^{3}	1.6×10^{2}	6.4:1
1.0×10^{20}	2.048×10^{3}	2.1×10^{2}	9.8:1
1.0×10^{78}	2.1×10^{4}	6.0×10^{2}	35.0:1

其中，破解时间的单位为 MIPS 年，密钥长度的单位为 bit。从表 1 可知，RSA/DSA 密码体制要求的密钥长度为 1024 比特时才能够达到安全需要，而对于 ECC 密码体制 160 比特就已经足够满足安全需要。而且当密钥长度增加时，ECC 密码算法的安全强度要比 RSA 密码体制和 DSA 密码体制的安全强度增加快得多，例如密钥长度为 210 比特的 ECC 密码算法要比 2048 比特的 RSA 密码算法和 DSA 密码算法安全，此时 RSA 密码算法和 DSA 密码算法的密钥长度从 1024 比特增加到了 2048 比特，而 ECC 密码算法的密钥长度仅仅从 160 比特增加到 210 比特。因此，相对于 RSA/DSA 等其它公钥密码系统，椭圆曲线密码体制具有安全强度高、运算量小、密钥长度短、运算速度快、所需带宽少等优点[9] ，这使得 ECC 密码体制逐步成为公钥密码系统的主流加密技术成为必然趋势。

4 结束语

椭圆曲线密码体制是建立在椭圆曲线数学理论基础之上的公钥密码系统，它是一种安全强度高、计算量

(下转第 234 页)

目标网络及时有效的监控。丢包率之所以低主要有 3 方面原因:

1. 本系统采用 NAPI 机制来实现基于 Libpcap 的捕包机制;

2. 测试环境流量虽然有近千兆,但是 DNS 数据量并不是很大,程序设计为丢弃除 DNS 数据包的所有数据包;

3. 用于测试的系统硬件配置相对较高,可以最大程度的降低丢包率。

3 结束语

针对 Web 通信的安全问题,文中提出了一套涉及分析、匹配以及控制的域名监控方案。设计的域名解析能够高效地捕获解析网络中的 DNS 报文获取域名信息,设计的匹配方案可以快速判断域名是否属于可疑或者非法域名,设计的安全控制模块能够重定向和阻断通信连接,从而在 Web 通信的第一步就防止了网络非法行为的产生,提供了网络的安全性。

参考文献:

[1] 国家互联网应急中心. 2011 年中国互联网网络安全报告[EB/OL]. [2011-04-22]. http://www.cert.org.cn/articles/docs/common/2011042225342.shtml.

[2] Mockapetris P. RFC1034-Domain names-concepts and facilities[S]. [s.l.]: Network Working Group,1987.

[3] 郑海涛. 基于网络信息内容的 DNS 检测系统的设计与实现[D]. 北京: 北京交通大学,2009.

[4] Ansari S,Rajeev S G,Chandrashekar H S. Packet sniffing: a brief introduction[J]. IEEE Potentials,2003,21(5):17-19.

[5] 万国根,秦志光,刘锦德. 网络内容安全分析及审计技术研究[J]. 计算机应用研究,2004,21(1):117-118.

[6] Stevens W R. UNIX 网络编程第一卷: 套接口 API[M]. 杨继张,译. 第 3 版. 北京: 清华大学出版社,2006.

[7] Liu Bin,Li Zhitang,Li Yao. High Speed Network Packet Capture Based on Linux[J]. Application Research of Computers,2006,23(5):225-227.

[8] 陶善旗,李 俊,郭伟群,等. 入侵检测系统中模式匹配算法的研究与改进[J]. 计算机技术与发展,2010,20(2):168-170.

[9] 孙晓妍,武东英,祝跃飞,等. Wu_Manber 多模式匹配算法的研究与改进[J]. 计算机工程,2008,34(8):85-89.

[10] Green I. DNS spoofing by the man in the middle[EB/OL]. 2005. http://www.sans.org/rr/whitepapers/dns/1567.php.

[11] 刘 扬,刘 杨,胡仕成,等. 基于 ARP 与 DNS 欺骗的重定向技术的研究[J]. 计算机工程与设计,2007,28(23):5604-5609.

[12] Andreasson O. Iptables-tutorial[EB/OL]. 2003. http://www.frozentux.net/documents/iptables-tutorial/.

(上接第 230 页)

小、占用存储空间小、所需带宽要求低的非对称加密算法,目前主要应用于快速加密解密、身份鉴别、数字签名认证、密钥信息交换、移动传输通信、智能卡安全等安全需求高的领域,所以椭圆曲线密码具有十分广阔的应用价值和理论研究意义。同时随着椭圆曲线密码理论的不断突破和新型技术的持续更新,椭圆曲线密码算法的实现速度也将会大幅提升,因而其安全性强度也将必然更高,所以椭圆曲线密码将是更适合于当今社会电子商务/政务和智能卡等需要安全和高效密码系统的加密算法,对于椭圆曲线密码的研究将会有更加广泛的应用前景和实际应用价值。

参考文献:

[1] Koblitz N. Elliptic curve cryptosystem[J]. Mathematics of Computation,1987,48(177):315-322.

[2] Miller V. Uses of elliptic curves in cryptography[C]//Advances in Cryptology-CRYPTO'85 Proceedings. [s.l.]: [s.n.],1986:417-426.

[3] 孟春岩,范 辉,余雪丽. 椭圆曲线用于加密的安全性讨论[J]. 微型机与应用,2001(6):59-60.

[4] 白国强,马润年,肖国镇. 化离散对数问题为特殊的椭圆曲线离散对数问题[J]. 西安电子科技大学学报,2001,28(2):254-257.

[5] 徐秋亮,李大兴. 椭圆曲线密码体制[J]. 计算机研究与发展,1999,36(11):1281-1288.

[6] Xu Guangwu. Short vectors,the GLV method and discrete logarithms[J]. Journal of Lanzhou University (Natural Sciences),2009,45(1):73-77.

[7] 杨君辉,戴宗铎,杨栋毅,等. 一种椭圆曲线签名方案与基于身份的签名协议[J]. 软件学报,2000,11(10):1303-1306.

[8] 黄建华,马大朋. 椭圆曲线密码体制理论与安全性分析[J]. 网络安全技术与应用,2008(7):91-93.

[9] 张晓丰,樊启华,程红斌. 密码算法研究[J]. 计算机技术与发展,2006,16(2):179-180.

[10] 张海波,王小非,夏学知,等. 一个改进的离散对数问题攻击算法[J]. 计算机应用,2007,27(4):843-845.

[11] 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):2116-2122.

[12] 孟春岩. 椭圆曲线加密算法密钥长度讨论[J]. 电力学报,2007,22(4):479-481.