文章编号：1672-2892(2003)02-0007-06

ECDSA 算法实现及其安全性分析

张 伟

（中国工程物理研究院 电子工程研究所，四川 绵阳 621900）

摘 要：阐述了 ANSI X9.62 椭圆曲线数字签名算法（ECDSA）基本原理；对其安全性进行了初步探讨；并根据该原理对 ECDSA 进行了程序实现；通过对该程序的运行分析与测试表明，该程序实现了 ECDSA 的基本功能，且具有系统参数小、处理速度快、密钥尺寸小等优点。

关键词：椭圆曲线密码学；ECDSA；算法实现；安全性

中图分类号：TP393.08 文献标示码：A

1 前言

椭圆曲线密码系统(ECC)于 1985 年由 Neal Koblitz[1]和 Victor Miller[2]发明，可看作是传统离散对数(DL)密码系统的椭圆曲线对等表示。传统系统中的 Z^*_p 子群被有限域上的椭圆曲线点群所代替。椭圆曲线密码系统安全性的数学基础是椭圆曲线离散对数问题(ECDLP)的计算复杂性。

由于 ECDLP 比 DLP 困难得多，椭圆曲线系统中每个密钥位的强度在本质上要比传统的离散对数系统大得多[3]。因而除了具有相同等级的安全性外，ECC 系统所用的参数比 DL 系统所用的参数少。该系统的优点是参数少、速度快以及密钥和证书都较小。这些优点在处理能力、存储空间、带宽和能源受限的环境中尤其重要。本文阐述了 ANSI X9.62 ECDSA 算法及其软件实现，并对其安全性进行了初步探讨。

2 椭圆曲线数字签名算法基本原理简介

2.1 数字签名方案

数字签名方案用于提供手写体签名(或其它签名)的数字副本。数字签名是只有签名者才知道的一些秘密数字(签名者的私钥，该数字用来对消息内容进行签名)。签名必须是可以验证的——如果出现诸如某个成员是否签署某个文档的争执，则没有偏见的第三方不需要访问签名者的私钥就能公正地解决该问题[4]。

数字签名方案可用于提供如下基本密码学服务：消息完整性(确保消息不被以非授权或未知方式改变)，消息源可信(确保消息源和声明相同)以及抗抵赖性(确保成员不能否认先前的行为和委托)。ANSI X9.62 (ECDSA)表达为：当运用适当的控制时，该标准的技术提供消息源、消息内容的完整性，消息初始可信性和抗抵赖性[3]。

2.2 有限域

有限域由在 F 上具有二元操作的 F 元素的有限集组成，二元操作指满足某一算法特性的加法和乘法。有限域的阶是域中元素的数量。当且仅当 q 为素数次方时存在 q 阶有限域。如果 q 为素数次方，则本质上只有一个 q 阶有限域；这个域记为 F_q。有很多方法描述 F_q 中的元素。

如果($q=p^m$)，这里 p 为素数，m 为正整数，则 p 称为 F_q 的特征值，m 称为 F_q 的扩展阶。大部分标准指定将椭圆曲线密码学技术限定在奇素数阶($q=p$)或 2 的幂($q=2^m$)之内。

p 为一奇素数时，称为素数域的有限域 F_q，由具有相应算法操作特性的整数集{0，1，2，…，p-1}组成。

有限域 F_{2^m} 称为特征双有限域和二元有限域，可以看作是由 0 和 1 组成的有限域 F_2 上的 m 维向量空间。也就是 F_{2^m} 中存在 m 个元素 $\alpha_1,\alpha_2,\cdots,\alpha_{m-1}$，满足每个 $\alpha\in F_{2^m}$ 能用以下的形式唯一写出：$\alpha = a_0\alpha_0 + a_1\alpha_1 + \cdots + a_{m-1}\alpha_{m-1}$，

收稿日期：2003-01-09； 修回日期：2003-05-30

基金项目：国防科技预研基金资助项目(421050504-2)

作者简介：张 伟(1972－)，男，助研，工学硕士，主要从事机械工程 CAD/CAE 应用与网络信息安全技术研究。

这里 $a_i \in \{0,1\}$。

2.3 有限域上的椭圆曲线

在 ECC 中，我们关心的是某种特殊形式的椭圆曲线，即定义在有限域上的椭圆曲线。

2.3.1 F_p 上的椭圆曲线

令 $p>3$ 为素数，F_p 上的椭圆曲线由形如公式(1)的等式定义：

$$y^2 = x^3 + ax + b \tag{1}$$

这里 a，$b \in F_p$，且 $4a^3+27b^2 \neq 0 (\mathrm{mod}\ p)$。椭圆曲线的点集 $E(F_p)$由所有满足等式(1)的点(x, y)，$x \in F_p$，$y \in F_p$ 组成，包括被称之为无穷点的特殊点O。

对于椭圆曲线上的两点相加给出椭圆曲线上第三点，有一条规则，称之为弦切律。伴随这种加法操作，$E(F_p)$的点集形成了一个用O点作为标记的群。正是这个群被用来构造椭圆曲线密码系统。

加法律最好用几何解释。令 $P=(x_1, y_1)$且 $Q=(x_2, y_2)$是椭圆曲线 E 上两个截然不同的点，则 P 和 Q 的和，记为 $R=(x_3, y_3)$，定义如下：首先通过点 P 和 Q 作一条直线；这条直线与椭圆曲线交于第三点；则点 R 就是这个点关于 x-轴的映像，如图 1 所示。图中的椭圆曲线由两部分组成，象椭圆的图形和无穷曲线。

如果 $P=(x_1, y_1)$，则 P 的加倍为 $R=(x_3, y_3)$定义如下：首先做一条直线与椭圆曲线相切于点 P；这条直线与椭圆曲线交于第二点；则点 R 就是这个点关于 x-轴的映像，如图 2 所示。

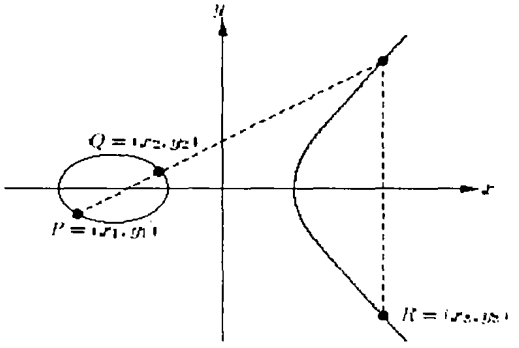

图 1 两个不同的椭圆曲线点相加的几何描述($P+Q=R$)

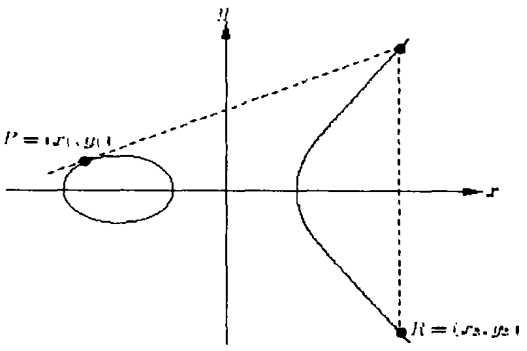

图 2 一个椭圆曲线点加倍的几何描述($P+P=R$)

2.3.2 F_{2^m} 上的椭圆曲线

F_{2^m} 上椭圆曲线由形如公式(2)的等式定义：

$$y^2 + xy = x^3 + ax^2 + b \tag{2}$$

这里 a，$b \in F_p$，且 $b \neq 0$，椭圆曲线的点集 $E(F_p)$由所有满足等式(2)的点(x, y)，$x \in F_p$，$y \in F_p$ 组成，这些点包括被称之为无穷点的特殊点O。

3 椭圆曲线数字签名的生成和验证算法

3.1 输入 ECDSA 域参数

ECDSA 的域参数由一条特征为 p 的有限域 F_q 上的椭圆曲线 E 和基点 $G \in E(F_q)$组成：

a) 域的大小 q，这里 $q=p$，为奇素数或 $q=2^m$；

b) 用一个描述指针 FR(域描述)描述 F_q 的元素；

c) 位串 seedE 的长度至少为 160 位；

d) F_q 上椭圆曲线 E 的等式定义的 F_q 上的两个元素 a 和 b；

e) 定义 $E(F_q)$中素数阶有限点 $G=(x_G, y_G)$的 F_q 上两个域元素 x_G 和 y_G；

f) 点 G 的阶数 n，$n>2^{160}$ 且 $n>4\sqrt{q}$；

g) 以及伴随因子 $h=\#E(F_q)/n$。

3.2 生成 ECDSA 密钥对

ECDSA 密钥对与 EC 域参数的特定集相关联。公钥是基点的随机倍数；而私钥则是用来生成这个倍数的整数。

为了生成 ECDSA 密钥对，每个成员 A 都要做如下操作(见图 3)：

a) 在区间[1，$n-1$]中选择一个随机或伪随机整数 d；

b) 计算 $Q=dG$；

c) A 的公钥是 Q，私钥是 d。

3.3 生成 ECDSA 签名

为了签署消息 m，具有域参数 $D=(q,\mathrm{FR},a,b,G,n,h)$ 及其相关密钥对 (d,Q) 成员 A 作如下操作(见图 4)：

a) 选择一个随机或伪随机整数 k 满足 $1\leqslant k\leqslant n-1$；

b) 计算 $kG=(x_1,y_1)$，且将 x_1 转换成整数 $\overline{x}_1$；

c) 计算 $r=x_1 \bmod n$，如果 $r=0$ 则回到第 a 步；

d) 计算 $k^{-1} \bmod n$；

e) 计算 SHA-1(m)，并将该位串转换成整数 e；

f) 计算 $s=k^{-1}(e+dr) \bmod n$，如果 $s=0$ 则回到第 a 步；

g) A 对消息 m 的签名为(r，s)。

3.4 验证 ECDSA 签名

要验证 A 在消息 m 上的签名为(r，s)，B 取得 A 域参数 D=(q,FR,a,b,G,n,h)的可信副本和相关公钥 Q，推荐 B 也验证 D 和 Q 的有效性，然后 B 做以下的操作(见图 5)：

a) 验证 r 和 s 是区间[1，$n-1$]内的整数；

b) 计算 SHA-1(m)，并将该位串转换成整数 e；

c) 计算 $w=s^{-1} \bmod n$；

d) 计算 $u_1=ew \bmod n$ 和 $u_2=rw \bmod n$；

e) 计算 $X=u_1G+u_2Q$；

f) 如果 $X=O$ 则拒绝签名；否则转换 X 的 x 坐标 x_1 为整数 $\overline{x}_1$，并计算 $v=\overline{x}_1 \bmod n$；

g) 当且仅当 $v=r$ 时接受签名。

4 椭圆曲线数字签名算法的程序实现

4.1 椭圆曲线数字签名算法的程序流程图

根据上述原理，用 C 语言开发了二元域 F_{2^m} 上的应用程序 ECDSA.exe。

4.1.1 椭圆曲线数字签名算法密钥对生成流程

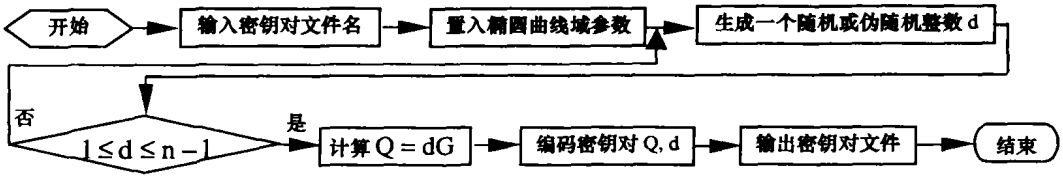

图 3　密钥对生成流程

4.1.2 椭圆曲线数字签名算法签名流程

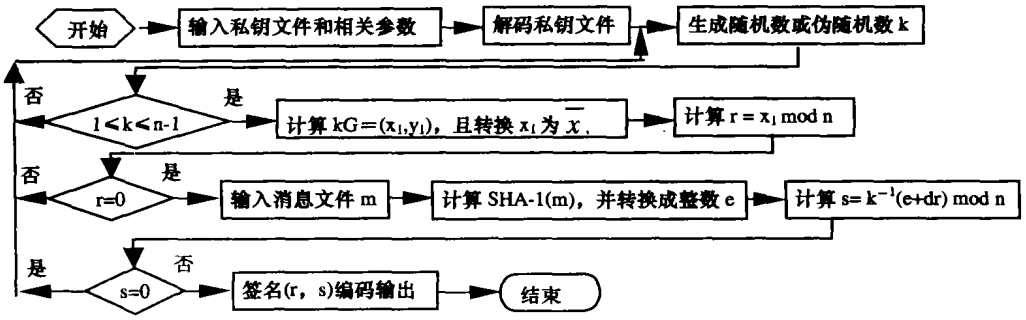

图 4 签名流程

4.1.3 椭圆曲线数字签名算法验证签名流程

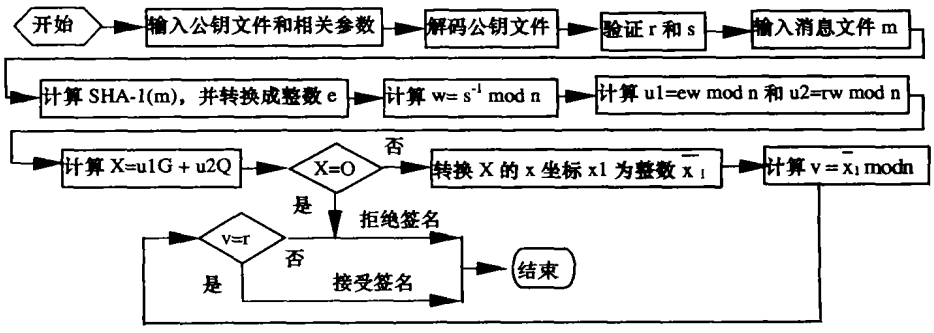

图 5 验证流程

4.2 椭圆曲线数字签名算法签名和验证实例

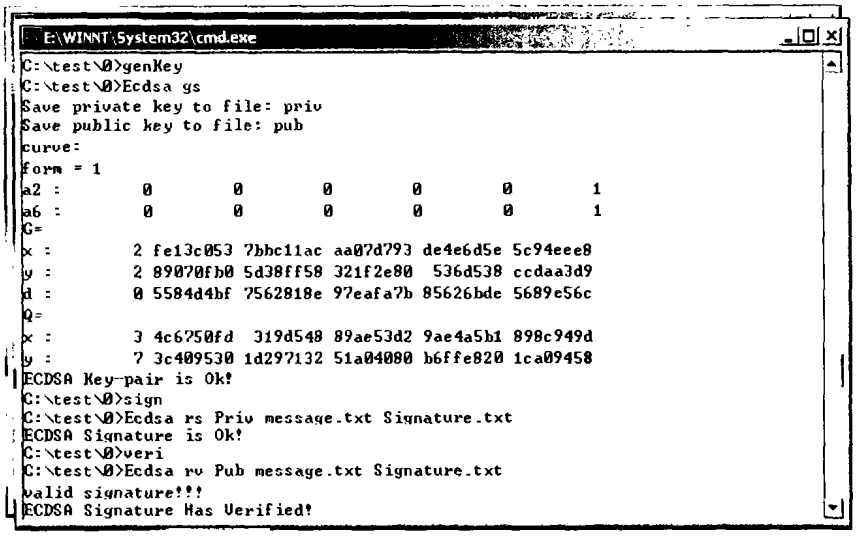

图6 ECDSA运行实例

a) 选用的 NIST 推荐椭圆曲线

m 163
FR Gaussian Normal Basis, T=4
a 0x00 00000000 00000000 00000000 00000000 00000001
b 0x00 00000000 00000000 00000000 00000000 00000001
xG 0x02 FE13C053 7BBC11AC AA07D793 DE4E6D5E 5C94EEE8
yG 0x02 89070FB0 5D38FF58 321F2E80 0536D538 CCDAA3D9
n 0x04 00000000 00000000 00020108 A2E0CC0D 99F8A5EF
h 2
FR2 约简多项式为 $f(x)= x^{163}+ x^{7}+ x^{6}+ x^{3}+1$

b) 私钥

0x0 0x5584d4bf 0x7562818e 0x97eafa7b 0x85626bde 0x5689e56c

c) 公钥

0x3 0x4c6750fd 0xa319d548 0x89ae53d2 0x9ae4a5b1 0x898c949d
0x7 0x3c409530 0x1d297132 0x51a04080 0xb6ffe820 0x1ca09450

d) 签名

437352739857664006357930435496927561584355920663 2
358259431021085487922441419420788324492992315909 3

e) 椭圆曲线数字签名密钥对生成、对消息文件签名以及验证签名的过程(如图6所示)。

f) ECDSA运行结果分析

由程序可知：签名有效输出为 Valid Signature；签名无效输出为 Invalid Signature。根据图 6 运行结果可以清楚看到该程序成功实现了密钥对生成、签名和验证过程。所以该程序基本完成了椭圆曲线数字签名算法的程序实现，结果正确。且由表 1 可知，该程序采用了 163 位推荐椭圆曲线,而目前可接受的安全强度为 112 位，所以该程序在密钥位的安全强度上是足够的。

5　椭圆曲线数字签名算法的安全性

ECDSA 的安全目标是，在现有软硬件条件下使用选择明文攻击签名不可伪造，对一个合法成员 A 发动此类攻击的攻击者的攻击目标是在获取 A 在攻击者所选择的消息集(不包括 m)上的签名之后，能获取 A 在某一单条消息上的有效签名。

当前流行的公钥密码系统的数学基础主要有以下三类[4]：

a) 因数分解问题(IFP)，如 RSA, Rabin-Williams 算法等；

b) 普通离散对数问题 (DLP)，如 DSA 算法；

c) 椭圆曲线离散对数问题 (ECDLP)，如 ECDSA 算法。

表 1 为不同密钥系统对密钥尺寸的需求，图 7 为几种公钥系统抗攻击性比较。从中可以看到对于相同的密钥位强度，ECC 系统要比其它几种公钥系统密钥尺寸小得多。

表 1　不同密钥系统对密钥尺寸的需求

RSA n	512*	1024	2048	3072	7680	15360
DSA p	512*	1024	2048	3072	7680	15360
ECC n	112*	161	224	256	384	512

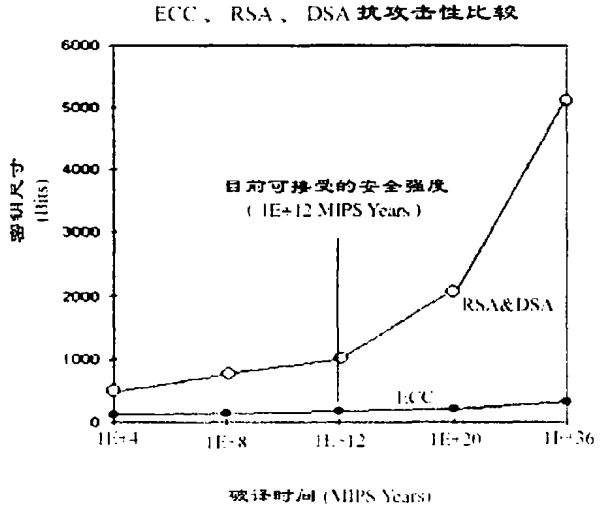

图 7　几种公钥系统抗攻击性比较

所以 ECC 和其它几种公钥系统相比，其抗攻击性具有绝对的优势，具有单位比特最高强度的安全性。如

160bit ECC 与 1024bit RSA、DSA 有相同的安全强度，而 224bit ECC 则与 2048bit RSA、DSA 具有相同的安全强度。鉴于 ECDSA 是 ECC 系统基本原理在数字签名中的应用，故 ECC 系统的安全性就是 ECDSA 的安全性。

Pointcheval 和 Stern[5]已经证明了，基于椭圆曲线离散对数问题且所使用的哈希函数是随机函数的前提下，对于选择明文攻击，ECDSA 在现有的情况下是不可伪造的。Brown[6]证明了在基本群为普通群且所使用的散列函数是抗冲突的前提下，ECDSA 本身是安全的。

6 结论

ECDSA是ANSI、IEEE、 FIPS、NIST和ISO标准，且正为其它的标准化组织作为标准。通过对其软件实现、运行测试及分析表明，它具有抗攻击性强、计算量小、处理速度快、密钥尺寸和系统参数小、带宽要求低等优点。所以研究开发具有自主知识版权的椭圆曲线数字签名算法对于提高信息安全水平有较大的实用价值和现实意义。

参考文献：

[1] N Koblitz. Elliptic curve cryptosystems[J]. Mathematics of Computation, 1987, (48): 203-209.
[2] V Miller. Uses of elliptic curves in cryptography [A]. Advances in Cryptology – Crypto'85, Lecture Notes in Computer Science[C], 1986,218: 387-398.
[3] Don B Johnson, Alfred J Menezes. Elliptic Curve Digital Signature Algorithm (ECDSA)[Z/OL]. http://www. certicom.com /resources/download/ecdsa.ps.
[4] (美)Bruce Schneier.应用密码学协议、算法与 C 程序[M].吴世中,等译.北京:机械工业出版社,2000.
[5] D Pointcheval, J Stern. Security proofs for signature schemes [A]. Advances in Cryptology-Eurocrypt '96, Lecture Notes in Computer Science[C], 1996, 1070: 417-426.
[6] M Brown. Software implementation of the NIST elliptic curves over prime fields[A]. Proceedings of RSA 2001[C], 2001.

The Algorithm Implementation of ECDSA and Security Analysis

ZHANG Wei
(Institute of Electronic Engineering, CAEP, Mianyang 621900,China)

Abstract: The arithmetic rationale of ANSI X9.62 Elliptic Curve Digital Signature Algorithm (ECDSA) is presented and its security is discussed preliminary. Through its program implementation and relative analysis it can be found that this program realizes the basic function of ECDSA and has much advantages like small parameters, fast computations and small key etc..

Key words: elliptic curve cryptography; ECDSA; algorithm implementation; security