基于有限域 GF (2^n)上圆锥曲线的公钥密码算法

蔡永泉, 赵 磊, 靳岩岩
(北京工业大学计算机学院, 北京 100022)

摘 要: 圆锥曲线密码学是一种新型的公钥密码学, 迄今对圆锥曲线密码学的研究成果都是以有限域 GF (p)上的圆锥曲线为基础的. 本文将有限域 GF (p)上的圆锥曲线 C (GF (p))推广为有限域 GF (2^n)上的圆锥曲线 C (GF (2^n)), 证明了圆锥曲线 C (GF (2^n))上的点和加法运算构成有限交换群 (C (GF (2^n)), ⊕), 并给出了圆锥曲线群 (C (GF (2^n)), ⊕)的阶的计算. 此外, 提出了使用有限域 GF (2^n)上的圆锥曲线群构造公钥密码系统, 并给出了 ElGamal加密方案和数字签名算法 (DSA)在圆锥曲线 C (GF (2^n))上模拟的算法, 最后分析其安全性.

关键词: 有限域 GF (2^n); 圆锥曲线; 公钥加密; 数字签名
中图分类号: TP309.7 文献标识码: A 文章编号: 0372-2112 (2006) 08-1464-05

A Public-Key Cryptosystem Based on Conic Curve in Finite Field *GF (2^n)*

CAI Yong-quan, ZHAO Lei, JIN Yan-yan
(College of Computer Science, Beijing University of Technology, Beijing 100022, China)

Abstract Conic curve cryptosystem was first introduced by CAO Zhenfu in 1998. By now, the previous study on conic curve cryptosystem has been based on conic curve group in finite field GF (p). Since the hardware circuits are suitable for performing addition, multiplication, squaring and the inversion operations in a finite field GF (2^n), the operations in finite field GF (2^n) are typically easier to implement in hardware and software than their counterpart in finite field GF (p). In order to speed up the computation of conic curve cryptosystem, the conic curve group is extended from finite field GF (p) to finite field GF (2^n), and the order of the conic curve group in finite field GF (2^n) is given. In addition, this paper suggests to use conic curve group in finite field GF (2^n) for realizing public-key cryptosystem, and presents the basic ElGamal public-key encryption scheme and the Digital Signature Algorithm (DSA) based on conic curve in finite field GF (2^n). Security of public-key cryptosystem based on conic curve in finite field GF (2^n) is analyzed.

Key words finite field GF (2^n); conic curve; public-key encryption; digital signature

1 引言

自从 Diffie和 Hellman提出公钥密码思想以来, 人们已经实现了多种公钥密码体制. 以椭圆曲线密码体制为代表、利用代数曲线构造的公钥密码算法受到了人们广泛的关注, 其中包括上世纪九十年代提出的圆锥曲线密码算法. 1998年, 曹珍富[1, 2]首先提出将圆锥曲线用于公钥密码算法, 利用有限域 GF (p)上圆锥曲线的点构成的群实现了圆锥曲线公钥密码系统, 并给出了 RSA算法在圆锥曲线上的模拟. 2001年, 戴宗铎等[3]指出有限域 GF (p)上的圆锥曲线群可以等价为一个有限域 GF (p^2)上普通乘群的子群. 2004年, 陆荣幸等[4 5]给出了基于圆锥曲线的门限签名方案和代理签名方案. 2005年, 孙崎等[6]详细说明了圆锥曲线群在环 Z_n 上的实现, 并在其上模拟了 KMOV数字签名方案. 以上研究成果基于张明志[7]提出的有限域GF (p)上圆锥曲线群(C (GF (p)), ⊕), 由于在有限域 GF (2^n)上的各项运算更适宜软、硬件实现, 因此, 本文将有限域 GF (p)上的圆锥曲线密码算法推广到有限域 GF (2^n)上, 以提高圆锥曲线密码算法的运算速度.

2 有限域 *GF (p)* 上的圆锥曲线密码算法及分析

2.1 有限域 *GF (p)* 上的圆锥曲线密码算法

有限域 GF (p)上的圆锥曲线 C (GF (p))是指同余方程[7]:

收稿日期: 2006-02-08; 修回日期: 2006-04-12
基金项目: 国家 863高技术研究发展计划 (No. 2005AA147090); 北京市教委科技发展面上项目 (No. KM200610005001)

$C(GF(p)): y^2 \equiv ax^2 - bx \bmod p,\ a, b \in (GF(p), *)$ (1)

其中 p 是奇素数. 将 $y \equiv xt \pmod p$ 代入式(1), 则圆锥曲线 $C(GF(p))$ 的全部点表示为:

$$C(GF(p)): P = \{p(t) = (x, y) = (b(a - t^2)^{-1}, bt(a - t^2)^{-1}) \mid t \in GF(p),\ t^2 \neq a\} \cup \{p(\infty) = (0, 0)\} \quad (2)$$

其中 $(a - t^2)^{-1}$ 为 $(a - t^2)$ 在有限域 $GF(p)$ 上的乘法逆元.

在 $C(GF(p))$ 上定义加法运算 $\oplus$: ①对于 $P = p(t) \in C(GF(p))$, 满足 $p(t) \oplus p(\infty) = p(\infty) \oplus p(t) = p(t)$. ②设 $P_1 = p(t_1), P_2 = p(t_2), P_3 = p(t_3) \in C(GF(p))$ 且 $t_1, t_2 \neq \infty$, 定义 $P_1 \oplus P_2 = P_3$, 即 $p(t_1) \oplus p(t_2) = p(t_3)$, 其中

$$t_3 = \begin{cases} (t_1 + t_2 + a)(t_1 + t_2)^{-1} \bmod p, & \text{当 } t_1 + t_2 \neq 0 \bmod p \\ \infty, & \text{当 } t_1 + t_2 \equiv 0 \bmod p \end{cases} \quad (3)$$

$C(GF(p))$ 上点 $P = p(t)$ 的逆元记作 $-P$, $-P$ 也是 $C(GF(p))$ 上一点, 且 $-P = p(-t)$, $-p(\infty) = p(\infty)$.

在 $C(GF(p))$ 上定义点乘运算: 令 k 是一个整数且 $P = p(t) \in C(GF(p))$, 记

$$kP = kp(t) = \begin{cases} \underbrace{p(t) \oplus p(t) \oplus \cdots \oplus p(t)}_{k\text{个}}, & \text{当 } k > 0 \\ p(\infty), & \text{当 } k = 0 \\ (-k)p(-t), & \text{当 } k < 0 \end{cases} \quad (4)$$

特别的, $C(GF(p))$ 上的倍点运算: $P_1 = p(t_1), P_3 = p(t_3) \in C(GF(p))$, 则 $2P_1 = P_3$, 即 $2p(t_1) = p(t_3)$, 其中

$$t_3 = \begin{cases} (t_1^2 + a)(2t_1)^{-1} \bmod p, & \text{当 } 2t_1 \neq 0 \bmod p \\ \infty, & \text{当 } 2t_1 \equiv 0 \bmod p \end{cases} \quad (5)$$

文献[1]给出了圆锥曲线 $C(GF(2^n))$ 的点数 $\#C(GF(2^n))$ 的计算公式,

$$\#C(GF(p)) = \begin{cases} p - 1, & \text{当勒让德符号} \left(\frac{a}{p}\right) = 1 \\ p + 1, & \text{当勒让德符号} \left(\frac{a}{p}\right) = -1 \end{cases} \quad (6)$$

文献[7]中证明了圆锥曲线 $C(GF(p))$ 的点和加法运算构成群, 文献[1]提出了将明文嵌入圆锥曲线 $C(GF(p))$ 后, 利用圆锥曲线群 $(C(GF(p)), \oplus)$ 构造基于离散对数的密钥交换协议和公钥密码系统的方法, 如: Diffie-Hellman 密钥交换协议、ElGamal 加密方案和 Massey-Omura 加密方案等.

2.2 问题分析

因为有限域 $GF(2^n)$ 上的运算只涉及移位和按位的模 2 加法, 所以在有限域 $GF(2^n)$ 上进行圆锥曲线群的各项运算更适宜软件和硬件的实现. 若在有限域 $GF(2^n)$ 上直接使用圆锥曲线 $C(GF(p))$, 由于 $\forall t \in GF(2^n)$, $2t \equiv 0$, 则对于 $\forall P = p(t)$, 倍点规则 $2P \equiv p(\infty)$, 且点乘运算为:

$$kP = \begin{cases} p(t), & \text{当 } k \text{ 为奇数} \\ p(\infty), & \text{当 } k \text{ 为偶数} \end{cases} \quad (7)$$

显然, 圆锥曲线群仅存在阶为 2 的子群, 因此, 无法利用圆锥曲线上的点构造离散对数难题. 由此得到结论: 文献[7]中定义的圆锥曲线群 $(C(GF(p)), \oplus)$ 无法直接应用到有限域 $GF(2^n)$ 上, 需要重新定义有限域 $GF(2^n)$ 上的圆锥曲线 $C(GF(2^n))$ 及各项运算.

3 有限域 $GF(2^n)$ 上的圆锥曲线加密算法和数字签名

3.1 有限域 $GF(2^n)$ 上的圆锥曲线群

定义有限域 $GF(2^n)$ 上的圆锥曲线 $C(GF(2^n))$ 是指同余方程:

$$C(GF(2^n)): y^2 + xy \equiv ax^2 + bx \bmod f(x),\ a, b \in GF(2^n) \quad (8)$$

其中 $f(x)$ 是构造有限域 $GF(2^n)$ 的既约多项式, 次数 $n = \deg(f)$. 注意有限域 $GF(2^n)$ 上的"+"和"−"运算等效. 参照文献[7]引入参数 t, 其几何解释为原点 (0, 0) 和点 $P = p(t) \in C(GF(2^n))$ 所确定直线的斜率. 从而, 有限域 $GF(2^n)$ 上圆锥曲线的全部点表示为:

$$C(GF(2^n)): P = \{p(t) = (x, y) = (b(t^2 + t + a)^{-1}, bt(t^2 + t + a)^{-1}) \mid t \in GF(2^n),\ t^2 + t \neq a\} \cup \{p(\infty) = (0, 0)\} \quad (9)$$

其中 $(t^2 + t + a)^{-1}$ 为 $(t^2 + t + a)$ 在有限域 $GF(2^n)$ 上的乘法逆元, 可利用扩展欧几里得算法求解.

在 $C(GF(2^n))$ 上定义加法运算 $\oplus$: ①对于 $P = p(t) \in C(GF(2^n))$, 满足 $p(t) \oplus p(\infty) = p(\infty) \oplus p(t) = p(t)$. ②设 $P_1 = p(t_1), P_2 = p(t_2), P_3 = p(t_3) \in C(GF(2^n))$ 且 $t_1, t_2 \neq \infty$, 定义 $P_1 \oplus P_2 = P_3$, 即 $p(t_1) \oplus p(t_2) = p(t_3)$, 其中

$$t_3 = \begin{cases} (t_1 t_2 + a)(t_1 + t_2 + 1)^{-1} \bmod f(x), & \text{当 } t_1 + t_2 + 1 \neq 0 \\ \infty, & \text{当 } t_1 + t_2 + 1 = 0 \end{cases} \quad (10)$$

以下为式(10)的求解过程: 由定义可知 t_3 的几何意义为点 $p(t_1)$ 和点 $p(t_2)$ 所确定直线的斜率,

当 $t_1 + t_2 + 1 \neq 0$ 且 $t_1 \neq t_2$ 时,

$$t_3 = \frac{y_2 - y_1}{x_2 - x_1} \equiv (t_1 t_2 + a)(t_1 + t_2 + 1)^{-1} \bmod f(x) \quad (11)$$

当 $t_1 + t_2 + 1 \neq 0$ 且 $t_1 = t_2$ 时,

$$t_3 = y'_x = \frac{2ax + b - y}{x + 2y} \equiv (t_1^2 + a)(2t_1 + 1)^{-1} \bmod f(x) \quad (12)$$

当 $t_1 + t_2 + 1 = 0$ 时, $t_3 = \infty$ (13)

将式(11-13)综合起来便得到了式(10). $C(GF(2^n))$ 上点 $P = p(t)$ 的逆元记作 $-P$, $-P$ 也是 $C(GF(2n))$ 上一点, 且 $-P = p(t + 1)$, $-p(\infty) = p(\infty)$.

在 $C(GF(2^n))$ 上定义点乘运算: 令 k 是一个整数且 $P = p(t) \in C(GF(2^n))$, 记

$$kP = kp(t) = \begin{cases} \underbrace{p(t) \oplus p(t) \oplus \cdots \oplus p(t)}_{k\text{个}}, & \text{当 } k > 0 \\ p(\infty), & \text{当 } k = 0 \\ (-k)p(t + 1), & \text{当 } k < 0 \end{cases} \quad (14)$$

定理 1 基于有限域 $GF(2^n)$ 的圆锥曲线 $C(GF(2^n))$ 上的点和加法运算 $\oplus$ 构成一个有限交换群 $(C(GF(2^n)), \oplus)$.

证明 (Ⅰ)有限群: 因为 $C(GF(2^n))$定义在有限域 $GF(2^n)$上, 所以圆锥曲线上点的个数是有限的;

(Ⅱ)单位元: 由 $C(GF(2^n))$上定义的加法运算 $\oplus$可知 $p(\infty)$对应原点 $(0,0)$为单位元;

(Ⅲ)逆元存在且唯一: 由式(10)可知, 当 $t_1+t_2+1=0$ 时, $p(t_1)\oplus p(t_2)=p(\infty)$. 由于 t_1 与 t_2 一一对应、$p(t_1)$与 t_1 一一对应、$p(t_2)$与 t_2 一一对应, 因此 $p(t_2)$与 $p(t_1)$一一对应, 即对于 $\forall P=p(t)\in(C(GF(2^n)))$有且仅有一个逆元;

(Ⅳ)封闭性: 由于圆锥曲线 $C(GF(2^n))$上的点和加法运算 $\oplus$完全定义在有限域 $GF(2^n)$上, 因此, 有限域 $GF(2^n)$的封闭性保证了圆锥曲线 $C(GF(2^n))$上运算的封闭性;

(Ⅴ)结合律: 即证明 $(p(t_1)\oplus p(t_2))\oplus p(t_3)=p(t_1)\oplus(p(t_2)\oplus p(t_3))$,

(1)当 $p(t_1)$, $p(t_2)$, $p(t_3)$中至少一个为 $p(\infty)$时, 显然, 命题成立;

(2)当 $p(t_1)$, $p(t_2)$, $p(t_3)\neq p(\infty)$时, 由于 $p(t_2)$与 $p(t_1)$、$p(t_3)$进行 $\oplus$运算, 因此, 以 $p(t_2)$为参考对象, 讨论 $p(t_2)$仅与 $p(t_1)$互逆、$p(t_2)$仅与 $p(t_3)$互逆、$p(t_2)$与 $p(t_1)$和 $p(t_3)$都互逆、$p(t_2)$与 $p(t_1)$和 $p(t_3)$都不互逆四种情况:

(a)当 $p(t_2)$仅与 $p(t_1)$互逆时, 即 $p(t_1)\oplus p(t_2)=p(\infty)$, 则 $(p(t_1)\oplus p(t_2))\oplus p(t_3)=p(t_3)$. 由于 $p(t_1)$与 $p(t_2)$互逆, 所以 $p(t_1)$与 $(p(t_2)\oplus p(t_3))$不互逆, 且由式(10)可知 $t_1+t_2+1=0$, 则

$$\begin{aligned}&p(t_1)\oplus(p(t_2)\oplus p(t_3))\\&=p((t_1t_2t_3+a(t_1+t_2+t_3)+a)(t_1t_2+t_2t_3+t_1t_3+t_1+t_2+t_3+a+1)^{-1})\\&=p((t_1t_2t_3+at_3+a(t_1+t_2+1))(t_1t_2+t_3(t_1+t_2+1)+(t_1+t_2+1)+a)^{-1})\\&=p((t_1t_2t_3+at_3)(t_1t_2+a)^{-1})=p(t_3)\end{aligned}$$

(b)当 $p(t_2)$仅与 $p(t_3)$互逆时, 与(a)同理, 命题成立;

(c)当 $p(t_2)$与 $p(t_1)$和 $p(t_3)$都互逆时, 由逆元唯一性可知 $p(t_1)=p(t_3)$, 显然命题成立;

(d)当 $p(t_2)$与 $p(t_1)$和 $p(t_3)$都不互逆时,

$$\begin{aligned}&(p(t_1)\oplus p(t_2))\oplus p(t_3)\\&=(p(t_1t_2+a)(t_1+t_2+1)^{-1})\oplus p(t_3)\\&=p(((t_1t_2+a)(t_1+t_2+1)^{-1}t_3+a)((t_1t_2+a)(t_1+t_2+1)^{-1}+t_3+1)^{-1})\\&=p((t_1t_2t_3+a(t_1+t_2+t_3)+a)(t_1t_2+t_2t_3+t_1t_3+t_1+t_2+t_3+a+1)^{-1})\end{aligned}$$

同理,

$$\begin{aligned}&p(t_1)\oplus(p(t_2)\oplus p(t_3))\\&=p((t_1t_2t_3+a(t_1+t_2+t_3)+a)(t_1t_2+t_2t_3+t_1t_3+t_1+t_2+t_3+a+1)^{-1})\end{aligned}$$

综上所述: $(p(t_1)\oplus p(t_2))\oplus p(t_3)=p(t_1)\oplus(p(t_2)\oplus p(t_3))$.

(Ⅵ)交换律:

(1)当 $p(t_1)$, $p(t_2)$中至少一个为 $p(\infty)$时, $p(t_1)\oplus p(t_2)=p(t_2)\oplus p(t_1)$;

(2)当 $p(t_1)$, $p(t_2)\neq p(\infty)$时,

$$\begin{aligned}p(t_1)\oplus p(t_2)&=p((t_1t_2+a)(t_1+t_2+1)^{-1})\\&=p((t_2t_1+a)(t_2+t_1+1)^{-1})\\&=p(t_2)\oplus p(t_1).\end{aligned}$$

引理 **1** 若 t, $a\in GF(2^n)$, $f(x)$为构造 $GF(2^n)$的既约多项式, 则 $t_2+t\equiv a \bmod f(x)$或无解或有两个不同余的解.

证明 (Ⅰ)方程有且仅有两个解:

由于 a的取值为 $GF(2^n)$上的任意值, 所以 $t^2+t=t(t+1)\equiv a \bmod f(x)$一定存在有解的情况.

(1)有两个解: 若 $t(t+1)\equiv a \bmod f(x)$存在解 t_1, 即 $t_1(t_1+1)\equiv a \bmod f(x)$. 那么当 $t_2=(t_1+1)\bmod f(x)$时, $t_2(t_2+1)=(t_1+1)(t_1+2)=(t_1+1)t_1\equiv a \bmod f(x)$. 因此, t_2 也为 $t(t+1)\equiv a \bmod f(x)$的解.

(2)仅有两个解: 反证法. 当 $t_1\neq t_2\neq t_3$时, 假设 t_3 为方程的第 3个解, 则

$$\begin{aligned}t_1^2+t_1=t_3^2+t_3&\equiv a \pmod{f(x)}\\t_1^2-t_3^2+t_1-t_3&\equiv 0 \pmod{f(x)}\\(t_1-t_3)(t_1+t_3+1)&\equiv 0 \pmod{f(x)}\\t_3=-(t_1+1)&=t_1+1=t_2\end{aligned}$$

与条件矛盾, 假设不成立.

(Ⅱ)方程存在无解的情况: 由 t 可值 $GF(2^n)$上的任意值和一组解 (t_1,t_2)对应一个 a, 可知 t只能确定 2^{n-1}个 a 的值. 但是 a在 $GF(2^n)$上的取值个数为 2^n 个, 因此, 另外 2^{n-1}个 a 的取值使得 $t^2+t\equiv a \bmod f(x)$无解.

定理 **2** 有限域 $GF(2^n)$上的圆锥曲线 $C(GF(2^n))$的点数, 即圆锥曲线群 $(C(GF(2^n)),\oplus)$的阶为 $\#C(GF(2^n))$, 则

$$\#C(GF(2^n))=\begin{cases}2^n-1, & \text{当 } t^2+t\equiv a \bmod f(x)\text{有解}\\2^n+1, & \text{当 } t^2+t\equiv a \bmod f(x)\text{无解}\end{cases}$$

证明 由式(9)和引理 1可知, 当 $t^2+t\equiv a \bmod f(x)$无解时, t的取值为有限域 $GF(2^n)$上的任意值和 ∞, 所以圆锥曲线 $C(GF(2^n))$上点的个数为 2^n+1; 而当 $t^2+t\equiv a \bmod f(x)$有解时(两个解), t的取值为有限域 $GF(2^n)$上 $t^2+t\neq a \bmod f(x)$的值和 ∞, 所以圆锥曲线 $C(GF(2^n))$上点的个数为 $2^n-2+1=2^n-1$.

3.2 明文嵌入

利用圆锥曲线群 $(C(GF(2^n)),\oplus)$构造密码算法时, 需要将明文表示为圆锥曲线 $C(GF(2^n))$上点的形式, 即明文嵌入. 当需要将明文 m 变换为点 $M=p(m)$的形式时, 编码算法为 $m\rightarrow p(m)$, 解码算法为 $p(m)\rightarrow m$; 当需要将明文 m 变换为点 $M=(x,y)$的形式时, 编码算法为 $m\rightarrow(x_m,y_m)=(b(m^2+m+a)^{-1},lm(m^2+m+a)^{-1})$, 解码算法为 $y_mx_m^{-1}\rightarrow m$.

3.3 有限域 $GF(2^n)$上的圆锥曲线加密算法

圆锥曲线上的离散对数难题是所有圆锥曲线公钥密码算法的安全性基础, 利用这一离散对数难题, 可以在圆锥曲线 C (GF (2^n))上实现 ElGamal和 Massey-Omura等公钥加密方案. 算法 1给出了 ElGamal加密方案在圆锥曲线 C (GF (2^n)上模拟的算法, 其中实体 A 为信息接收者、实体 B为信息发送者. 例 1给出了在人为小参数的前提下, 利用有限域 GF (2^4) 上的圆锥曲线实现 ElGamal加密方案的例子.

算法 **1**　ElGamal加密方案在圆锥曲线 C (GF (2^n)上的实现

step 1　系统的建立: (1)选择有限域 GF (2^n) 和既约多项式 f(x); (2)随机选择一条定义在有限域GF (2^n)上的圆锥曲线C (GF (2^n); (3)选择圆锥曲线 C (GF (2^n) 上一点 P = p (g), 点 P 的阶为 ord(P).

step 2　密钥的生成: 实体 A 执行下列步骤: (1)随机选取整数 d∈ [0, ord(P) - 1], 将 d 作为私钥; (2)计算点 Q = p (q) = dP = dp (g), 将Q 作为公钥.

step 3　加密过程: 当实体 B发送明文m 给实体 A 时, B执行下列步骤: (1)将明文 m 编码为M = p (m) 的形式; (2)查找实体 A 的公钥 Q; (3)随机选择整数 k∈ [0, ord (P) - 1]; (4)计算密文 $c_1 = kP = kp(g)$; (5)计算密文 $c_2 = M \oplus (kQ) = p(m) \oplus (kp(q))$; (6)传送密文 (c_1, c_2) 给实体 A.

step 4　解密过程: 当实体 A解密从实体 B 收到的密文 (c_1, c_2)时, A 执行下列步骤: (1)计算点 dc_1; (2)计算点 dc_1 的逆元 $-(dc_1)$; (3)恢复数据 $p(m) = c_2 \oplus (-(dc_1))$; (4)将 p (m)解码为明文m.

例 **1**在有限域 GF (2^4)的圆锥曲线上实现 ElGamal加密方案的例子.

step 1　系统的建立: (1)既约多项式 $f(x) = x^4 + x + 1$; (2)选择 C (GF (2^4)): $(0001)y^2 + (0001)xy = (1001)x^2 + (1000)x$; (3)选择点 P = p (g) = p (0010), 由于 17P = p (∞), 故点 P 的阶 ord (P) = 17.

step 2　密钥的生成: 实体 A 执行下列步骤: (1)选取区间 [1, 16]中一个随机整数 d = 2, 将d 作为私钥; (2)计算点 Q = p (q) = dp (g) = 2p (0010) = p (1101), 将Q 公开.

step 3　加密过程: 当实体 B发送明文 m = 0011 给实体 A时, B执行下列步骤: (1)编码 $m \rightarrow p(m) = p(0011)$; (2)查找A 的公钥Q = p (1101); (3)在区间 [1, 16]中选取一个随机整数 k = 5; (4)计算密文 $c_1 = kP = kp(g) = 5p(0010) = p(0101)$; (5)计算密文 $c_2 = M \oplus (kQ) = p(m) \oplus (kp(q)) = p(1011) \oplus (5p(1101)) = p(0011) \oplus p(1011) = p(1110)$; (6)传送密文 $(c_1, c_2) = (p(0101), p(1110))$ 给实体 A.

step 4　解密过程: 当实体 A解密从实体 B 收到的密文 (p(0101), p (1110))时, 实体 A 执行下列步骤: (1)计算点 $dc_1 = 2p(0101) = p(1011)$; (2)计算点 $-(dc_1) = p(1011 + 0001) = p(1010)$; (3)恢复数据 $p(m) = c_2 \oplus (-(dc_1)) = p(1110) \oplus p(1010) = p(0011)$; (4)解码 $p(m) \rightarrow m = 0011$.

3.4　有限域 GF(2^n)上的圆锥曲线数字签名

利用圆锥曲线上的离散对数难题, 在圆锥曲线 C (GF (2^n))上实现数字签名算法 (DSA), 它是 ElGamal和 Schorr签名算法的变型. 该算法需要将待签名的消息利用杂凑函数 H 变换成一个固定长度的消息摘要, 然后对摘要进行签名, 签名的验证需要签名数据和原始消息. 算法 2给出了 DSA 在圆锥曲线 C (GF (2^n))上模拟的数字签名算法, 其中实体 A 为签发者、实体 B 为验证者. 例 2给出了在人为小参数的前提下, 利用有限域 GF (2^4) 上的圆锥曲线实现 DSA 的例子.

算法 **2**　DSA 在圆锥曲线 C (GF (2^n)上的实现

step 1　系统的建立: (1)选择有限域 GF (2^n) 和既约多项式 f(x); (2)随机选择一条定义在有限域GF (2^n)上的圆锥曲线C (GF (2^n); (3)选择圆锥曲线 C (GF (2^n) 上一点 P = p (g), 点 P 的阶为 ord (P).

step 2　密钥的生成: 实体 A 执行下列步骤: (1)随机选取整数 d∈ [0, ord(P) - 1], 将 d 作为私钥; (2)计算点 Q = p (q) = dP = dp (g), 将Q 作为公钥.

step 3　数字签名: 实体 A 对信息 m 签名时将执行下列步骤: (1)随机选取整数 k∈ [0, ord(P) - 1]; (2)计算点 Z = p (z) = kP; (3)将 z 表示为整数 $\bar{z} = 7$; (4)计算 e = H (m); (5)签名 $r = \bar{z} \bmod ord(P)$; (6)签名 $s = k^{-1}(e + rd) \bmod ord(P)$; (7)信息 m 上的签名是 (r, s).

step 4　签名验证: 实体 B 验证信息 m 上的签名 (r, s) 时, 将执行下列步骤: (1)查找 A 的公钥 Q; (2)计算 e = H (m); (3)计算 $\omega = s^{-1} \bmod ord(P)$; (4)计算 $u_1 = e\omega \bmod ord(P)$; (5)计算 $u_2 = r\omega \bmod ord(P)$; (6)计算点 $Z' = p(\vec{z}) = u_1P \oplus u_2Q = u_1p(g) \oplus u_2p(q)$; (7)将 z'表示为整数; (8)计算 $v = \vec{z} \bmod ord(P)$; (9)若 v = r, 返回“接受签名”, 否则, 返回“拒绝签名”.

以上算法满足以下关系:

(1)杂凑函数 H 要求为抗原象攻击和抗碰撞的; (2)$r \neq 0$, 如果 r = 0, 则签名 $s = k^{-1}(e + rd)$不包含私钥 d; (3)如果 n 值足够大、k 是随即选取的, 则 r = 0或 s = 0的概率小的微乎其微.

例 **2**　实体 A 签名信息 m = 11100011010111100, 假设 m 通过杂凑函数 H 变换为 e = H (m) = 2, 其系统建立时的基本参数与例 1相同.

step 1, 2　系统建立、密钥生成的过程与例 1相同.

step 3　数字签名: A 执行下列步骤: (1)在区间 [1, 16]内选取一个随机整数 k, 如 k = 4; (2)计算点 Z = p (z) = 4P = 4p (0010) = p (0111); (3)将 z = (0111)表示为整数 $\bar{z} = 7$; (4)计算 e = H (m) = 2; (5)签名 $r = \bar{z} \bmod 17 = 7$; (6)签名 $s = k^{-1}(e + rd) \bmod ord(P) = 13(2 + 7 * 2) \bmod 17$

= 4, (7)信息 m 上的签名是 (r, s) = (7, 4).

step 4 签名验证: 实体 B如下验证信息 m 上的签名 (7, 4): (1)查找 A 的公钥 Q = p(1101); (2)计算 e = H(m) = 2; (3)计算 $\omega = 4^{-1} \bmod 17 = 13$; (4)计算 $u_1 = e\omega \bmod \mathrm{ord}(P) = 2 * 13 \bmod 17 = 9$; (5)计算 $u_2 = r\omega \bmod \mathrm{ord}(P) = 7 * 13 \bmod 17 = 6$; (6)计算 $Z' = p(z') = u_1 P \oplus u_2 Q = p(1110) \oplus p(0100) = p(0111)$; (7)将 z′表示为整数 $\overrightarrow{z'} = 4 + 2 + 1 = 7$; (8)计算 $v = \overrightarrow{z'} \bmod 17 = 7$; (9)因为 r = v, 故实体 B 接受签名.

3.5 安全性

圆锥曲线上的离散对数问题是指给定有限域上的圆锥曲线 C, 基点 P∈C, 阶为 n, 集合 ⟨P⟩是由点 P 生成的圆锥曲线循环子群, 点 Q∈⟨P⟩, 寻找一个整数 k∈[0, n − 1]使得 Q = kP. 整数 k 称为 Q 基于 P 的离散对数, 表示为 k = $\log_P Q$. 圆锥曲线上离散对数问题的困难性是所有圆锥曲线密码算法安全性的基础.

文献[1]中指出对于有限域 GF(p)上的圆锥曲线群 (C(GF(p))), 在点 P 有足够大的阶时, 求解有限域 GF(p)上圆锥曲线的离散对数问题是困难的, 即给定 k 和 P 计算 Q 相对容易, 但是给定 Q 和 P 确定 k 就相对困难(计算上不可行), 从而得到此算法的安全性.

由式(6)可知, 圆锥曲线 C(GF(p))的阶一定为偶数, 以 $\left(\frac{a}{p}\right) = -1$为例, 此时圆锥曲线 C(GF(p))的阶为 p + 1, 其中一定包含阶为 2, (p + 1)/2的子群. 最好的情况为 (p + 1)/2是素数, 即圆锥曲线群 (C(GF(p))仅包含阶为 2, (p + 1)/2和 (p + 1)的子群; 最坏的情况为 p 恰巧为梅森素数 (如 M_{1279}), 即圆锥曲线群 (C(GF(p))包含阶为 2, 4, 8……的子群. 显然, 小阶数子群中的元素是有一定数量的, 当选择这些元素为基点时, 会影响所构造密码算法的安全性.

由定理 2可知, 圆锥曲线 (C(GF(2^n)))的阶一定为奇数. 以 $t^2 + t \equiv a \pmod{f(x)}$无解为例, 此时圆锥曲线群 C(GF($2^n$))的阶为 ($2^n$ + 1). 最好的情况为(2^n + 1)为素数时, 即圆锥曲线群 (C(GF(2^n)))仅包含阶为 (2^n + 1)子群, 此时圆锥曲线 C(GF(2^n))上除原点 p(∞)外的任意点均为该群的生成元; 最坏的情况是 (2^n + 1)为 3的幂, 即包含 3, 9, 27……的子群. 因此, 在有限域中元素数量相同的条件下, 圆锥曲线(C(GF(2^n)))比圆锥曲线 (C(GF(p)))有略多可供选择的安全基点.

4 结束语

本文定义了有限域 GF(2^n)上圆锥曲线 C(GF(2^n))及各项运算, 证明了圆锥曲线 C(GF(2^n))上的点和加法运算 ⊕构成有限交换群 (C(GF(2^n)), ⊕), 同时给出了圆锥曲线 C(GF(2^n))上的点数, 即圆锥曲线群 (C(GF(2^n)), ⊕)的阶的计算公式. 最后, 提出了 ElGamal加密方案和数字签名算法(DSA)在圆锥曲线群 (C(GF(2^n))), ⊕)上模拟的算法, 并分别举例说明了在人为小参数的前提下两个算法的计算过程.

参考文献:

[1] 曹珍富. 基于有限域 F_p 上圆锥曲线的公钥密码系统[A]. 刘木兰等, 编, 第五届中国密码学学术会议论文集[C]. 北京: 科学出版社, 1998. 45−49.

[2] 曹珍富. RSA 与改进的 RSA 的圆锥曲线模拟[J]. 黑龙江大学自然科学学报, 1999, 16(4): 15−18.
Cao Zhen-fu. Conic analog of RSA cryptosystem and some improved RSA cryptosystems[J]. Journal of Natural Science of Heilongjiang University, 1999, 16(4): 15−18. (in Chinese)

[3] Dai Zongduo, Ye Dingfeng, Pei Dingyi, et al. Cryptanalysis of ElGamal type encryption schemes based on conic curves[J]. Electronics Letters, 2001, 37(7): 426.

[4] Lu Rongxing, Cao Zhenfu, Zhou Yuan. Threshold undeniable signature scheme based on conic[J]. Applied Mathematics and Computation, 2005, 162(1): 165−177.

[5] Lu Rongxing, Cao Zhenfu. A proxy-protected signature scheme based on conic[A]. Proceedings of the 3rd International Conference on Information Security[C]. New York: ACM Press, 2004. 22−26.

[6] 孙琦, 朱文余, 王标. 环 Z_n 上圆锥曲线和公钥密码协议[J]. 四川大学学报(自然科学版), 2005, 42(3): 471−478.
Sun Qi, Zhu Wen-yu, Wang Biao. The Conic Curves over Zn and Public-Key Cryptosystem Protocol[J]. Journal of Sichuan University (Natural Science Edition), 2005, 42(3): 471−478. (in Chinese)

[7] 张明志. 用圆锥曲线分解整数[J]. 四川大学学报(自然科学版), 1996, 33(4): 356−359.
Zhang Ming-zhi. Factoring Integers with Conics[J]. Journal of Sichuan University (Natural Science Edition), 1996, 33(4): 356−359. (in Chinese)

作者简介:

蔡永泉 男, 1956年生于安徽肥东, 博士、副教授, 主要研究方向为信息安全、计算机网络. E-mail: cyq@bjut.edu.cn

赵 磊 男, 1982年生于北京, 硕士研究生, 主要研究方向为信息安全.

靳岩岩 男, 1982年生于北京, 硕士研究生, 主要研究方向为信息安全.