二元 Edwards 曲线的半分算法*

林齐平[1],张方国[1,2]
(1. 中山大学 信息科学与技术学院,广东 广州 510006;
2. 中国科学院 软件研究所,北京 100190)

摘 要:利用二元 Edwards 曲线加法公式的对称性得到可做半分的公式。在推导半分算法过程中曲线参数有两种情况:$d_1 \neq d_2$ 和 $d_1 = d_2$。当曲线参数 $d_1 \neq d_2$ 时,利用和 Weierstrass 曲线的双有理等价关系、迹函数和半迹函数,得到了 Edwards 曲线的半分算法。而当曲线参数 $d_1 = d_2$ 时,给出了定理证明,虽然在这种情况下倍加公式更简单,但半分算法反而更复杂。进一步分析了半分算法的效率,指出虽然在二元 Edwards 曲线上可以进行半分运算,但目前半分算法的效率仍然比不上倍加方法。利用 ω - 坐标简化半分算法并应用在标量乘计算上。

关键词:点半分;二元 Edwards 曲线;ω - 坐标
中图分类号:TP309 **文献标志码**:A **文章编号**:1001 - 2486(2012)02 - 0021 - 04

Halving on binary Edwards curves

LIN Qiping[1], *ZHANG Fangguo*[1,2]
(1. School of Information Science and Technology, Sun Yat-sen University, Guangzhou 510006, China;
2. Institute of Software, Chinese Academy of Sciences, Beijing 100190, China)

Abstract: The formulas of binary Edwards curves which can be halved are transformed from the doubling ones by using the symmetry of the formulas. Two situations are to be handled in the derivation by the parameters of the curves. In the case of $d_1 \neq d_2$, it is naturally to get a halving algorithm by using the relation of birational equivalence from the Weierstrass curves, the trace functions and the half-trace functions. In the case of $d_1 = d_2$, a theorem is given to prove it. It is not easy to get a halving algorithm, although the doubling formulas are simpler in this case. Then the efficiency of the halving algorithm is analyzed. The result shows that the efficiency of the halving algorithm cannot catch up with that of the doubling one. Using the ω-coordinate, the halving algorithm is simplified, and is further used to compute the scalar multiplication.

Key words: point halving; binary Edwards curves; ω-coordinate

Edwards[1]在2007年提出一种新的椭圆曲线规范模型并给出了非二元域上的加法公式。同年 Bernstein 和 Lange[2]给出了 Edwards 曲线上的快速点加和倍加公式。不久 Bernstein 等[3]将 Edwards 点加公式推广到更一般的曲线上去。但这些公式不能用在特征为 2 的椭圆曲线上。Bernstein, Lange 和 Rezaeian Farashahi[4]介绍了一种计算二元 Edwards 曲线标量乘的新方法。他们分别用两种方法实现标量乘计算,一种采用传统的(X,Y,Z)坐标,另一种采用 ω - 坐标。

椭圆曲线密码学中最基础的运算是“倍加 - 点加”(double-and-add)算法。但从1999年开始,二元域上的椭圆曲线有等价的算法可以实现“倍加 - 点加”算法功能,该等价算法称为“半分 - 点加”算法。半分算法是由 Knudsen[5]和 Schroeppel[6]针对椭圆曲线二元域独立提出的。该算法是椭圆曲线密码学中有效算法之一。方法是对给定点 Q,从方程 $2P = Q$ 中解出点 P。它基于群元素的“对半”计算。在特征2上,半分算法比倍加算法运算速度快,因为在特征2的域上,计算平方根、迹函数或半迹函数都非常快。值得注意的是,在其他非特征2的域上计算半分算法不会比倍加算法快。

Knudsen[5]的主要工作是针对群的阶有因子2的曲线进行的。后来,King 和 Rubin[7]推广了 Knudsen 的半分算法到有因子 2^k ($k \geqslant 2$) 的曲线上。随后还有很多与半分算法相关的文献[8-12]。

1 二元 Edwards 曲线

定义1 (二元 Edwards 曲线[4]):设 k 是特

* **收稿日期**:2011 - 07 - 28
基金项目:国家自然科学基金资助项目(61070168,61003244)
作者简介:林齐平(1978—),男,广东揭阳人,博士研究生,E-mail:linqp@126.com;
张方国(通信作者),男,教授,博士,博士生导师,E-mail: isszhfg@mail.sysu.edu.cn

征为 2 的域，d_1, d_2 为 k 中两个元素且满足 $d_1 \neq 0$，$d_2 \neq d_1^2 + d_1$。以 d_1, d_2 为参数的二元 Edwards 曲线 E_{B,d_1,d_2} 如下：

$$d_1(x+y) + d_2(x^2+y^2) = xy + xy(x+y) + x^2y^2.$$

设 $(x_1, y_1), (x_2, y_2)$ 为 E_{B,d_1,d_2} 上两点，它们之和记为 (x_3, y_3)。令 $A = (x_1 + y_1)(x_2 + y_2)$，$B = (x_1 + x_2)$，$C = (y_1 + y_2)$，则点加公式如下：

$$x_3 = \frac{d_1 B + d_2 A + (x_1 + x_1^2)(x_2(C+1) + y_1 y_2)}{d_1 + (x_1 + x_1^2)(x_2 + y_2)},$$

$$y_3 = \frac{d_1 C + d_2 A + (y_1 + y_1^2)(y_2(B+1) + x_1 x_2)}{d_1 + (y_1 + y_1^2)(x_2 + y_2)}.$$

倍加公式如下：

$$x_3 = 1 + \frac{d_1 + d_2(x_1^2 + y_1^2) + y_1^2 + y_1^4}{d_1 + x_1^2 + y_1^2 + (d_2/d_1)(x_1^4 + y_1^4)},$$

$$y_3 = 1 + \frac{d_1 + d_2(x_1^2 + y_1^2) + x_1^2 + x_1^4}{d_1 + x_1^2 + y_1^2 + (d_2/d_1)(x_1^4 + y_1^4)}. \quad (1)$$

特别地，当 $d_1 = d_2$ 时倍加公式可以简化为

$$x_3 = \frac{d_1(x_1^2 + y_1^2) + x_1^2 + x_1^4}{d_1 + x_1^2 + y_1^2 + x_1^4 + y_1^4},$$

$$y_3 = x_3 + 1 + \frac{d_1}{d_1 + x_1^2 + y_1^2 + x_1^4 + y_1^4}. \quad (2)$$

本文只考虑反射坐标下的点加和倍加公式，射影坐标公式可以参考文献[4]。

利用 Montgomery 阶梯思想，Bernstein 等对二元 Edwards 曲线提出了基于 ω - 坐标的差分加法公式。“差分加法”表示对给定点 $(m+1)P$, mP, P，可以计算 $(2m+1)P$，或给定点 mP, mP, 0，计算 $2mP$。

令 (x_2, y_2) 为二元 Edwards 曲线 E_{B,d_1,d_2} 上一个点，并假设 $(x_4, y_4) = (x_2, y_2) + (x_2, y_2)$ 有定义。由二元 Edwards 曲线的定义我们可得到 $d_1^2 + d_1\omega_2^2 + d_2\omega_2^4 \neq 0$，其中 $\omega_i = x_i + y_i$，和公式

$$\omega_4 = \frac{\omega_2^2 + \omega_2^4}{d_1 + \omega_2^2 + (d_2/d_1)\omega_2^4}. \quad (3)$$

设 (x_1, y_1), $P = (x_2, y_2)$, $Q = (x_3, y_3)$, (x_5, y_5) 都是 E_{B,d_1,d_2} 上的点，并满足 $Q - P = (x_1, y_1)$ 和 $Q + P = (x_5, y_5)$，那么差分加法如下：

$$\omega_5 = \frac{\omega_2\omega_3(1 + \omega_2 + \omega_3) + (\omega_2\omega_3)^2}{d_1 + \omega_2\omega_3(1 + \omega_2 + \omega_3) + (d_2/d_1)(\omega_2\omega_3)^2} + \omega_1.$$

给定点 $Q - P$，$\omega(P)$ 和 $\omega(Q)$，从差分公式可以计算得到 $2P$。令 $E = \omega_1 + \omega_2$，$F = \omega_1\omega_2$，$G = \omega_2^2 + \omega_2$，如果 $\omega_1^2 + \omega_1 \neq 0$，那么

$$x_2^2 + x_2 = \frac{\omega_3(d_1 + F(E+1) + F^2 d_2/d_1) + d_1 E + (y_1^2 + y_1)G}{\omega_1^2 + \omega_1}.$$

类似地，给定 P，$\omega(mP)$，$\omega((m+1)P)$，可以计算 $2mP$。

2 半分算法（当 $d_1 \neq d_2$ 时）

设 E_{B,d_1,d_2} 的群的阶为 $2r$ 且 $E_{B,d_1,d_2}(F_{2^d}) = G \times E^{[2]}$，其中 r 和 d 为奇数。

令 $Q = (x_4, y_4) \in G$, $P = (x_2, y_2)$, $Q = 2P$ 并令 $\lambda = \frac{1}{d_1 + (x_2 + y_2)^2 + (d_2/d_1)(x_2 + y_2)^4}$。从倍加公式(1)可得

$$\begin{cases} x_4 = 1 + \lambda(d_1 + d_2(x_2 + y_2)^2 + y_2^2 + y_2^4), \\ y_4 = 1 + \lambda(d_1 + d_2(x_2 + y_2)^2 + x_2^2 + x_2^4). \end{cases} \quad (4)$$

上面两个方程相加可以得到 $\lambda(x_2 + y_2)^4 + \lambda(x_2 + y_2)^2 = x_4 + y_4$。把 λ 的值代入该式并令 $X_2 = x_2 + y_2$，$X_4 = x_4 + y_4$ 得到

$$(1 + (d_2/d_1)X_4)X_2^4 + (1 + X_4)X_2^2 = d_1 X_4. \quad (5)$$

2.1 半分公式

当 $X_4 + 1 = 0$ 或 $X_4 = d_1/d_2$ 时，方程(5)可以简化为 $X_2^4 = d_1/(1 + d_2/d_1)$ 或 $X_2^2 = d_1/(1 + d_2/d_1)$。从这两个方程中解出 X_2 只需平方根运算就可以。因此，下面我们假设 $X_4 \neq 1$ 和 d_1/d_2。现在，对给定的点 (x_4, y_4)，分析怎么用半分方法得到 (x_2, y_2)。

首先，设 $M = 1/(1 + X_4)(d_1/d_2 + X_4)$，$T = X_2^2$ 并代入方程(5)，得：

$$(d_1 + d_2X_4)T^2/d_1(1 + X_4) + T = X_4 d_1/(1 + X_4).$$

令 $T_1 = (1 + (d_2/d_1)X_4)T/(1 + X_4)$，上面的方程成为：

$$T_1^2 + T_1 = d_2 + d_1((d_1/d_2)M + MX_4) + (d_1 + d_2)((d_1/d_2)M + MX_4)^2. \quad (6)$$

下面我们求解该二次方程并判定哪一个解是正确的解。

引理 1 F_{2^d} 上的形如 $ax^2 + bx + c = 0 (a, b \neq 0)$ 的方程可以简化为 $T^2 + T = c'$ 的形式，并且该简化方程有解当且仅当 $\mathrm{Tr}(c') = 0$。若 d 为奇数，那么 $T^2 + T = c'$ 的一个根为半迹 $t = \sum_{i=0}^{(d-3)/2} c'^{2^{2i+1}}$，另一个根为 $t + 1$。

我们知道方程(6)有解，因为它是从方程(5)演化来的。这表示：

$\mathrm{Tr}(d_2 + d_1((d_1/d_2)M + MX_4) + (d_1 + d_2)((d_1/d_2)M + MX_4)^2) = 0$。并且存在两个根 t_1 和 $t_1 + 1$，下面我们将判定哪一个是正确的解。

取第一个根 t_1，可以得到值 t：$t = (d_1/d_2)(1 + (1 + d_1/d_2)(M + MX_4))t_1$.

可以由下面的迹函数 $\mathrm{Tr}(d_2+d_1/(1+X_2)+(d_1+d_2)/(1+X_2)^2)=0$ 判别哪一个是正确的解。这个迹函数可以进一步简化。因为对任何 $a\in F_{2^d}$ 都有 $\mathrm{Tr}(a^2)=\mathrm{Tr}(a)$ 成立[13]。这样如果迹函数 $\mathrm{Tr}(d_2(1+1/(1+t)))=0$ 成立,那么 t_1 就是正确的解。有了 t_1 和 t,我们可以计算得到 $X_2=\sqrt{t}$。反之,如果上述的迹函数的值不为 0,那么正确的解为 t_1+1,这时可以用下面的式子解出 X_2: $t=(d_1/d_2)(1+(1+d_1/d_2)(M+MX_4))(t_1+1)$, $X_2=\sqrt{t}$。

得到 X_2 之后,由方程(4)可以得到下面式子:$x_2^4+x_2^2+d_1+d_2X_2^2=(y_4+2)/\lambda$,即 $x_2^4+x_2^2=(y_4+1)(d_1+X_2^2+(d_2/d_1)X_2^4)+d_1+d_2X_2^2$。

令 $x_2'=x_2^2$,并代入上述方程,得:$x_2'^2+x_2'=(y_4+1)(d_1+X_2^2+(d_2/d_1)X_2^4)+d_1+d_2X_2^2$.

用半迹函数可以从该方程得到两个解。因此可得到 $x_2=\sqrt{x_2'}$ 或 $x_2=\sqrt{x_2'+1}$,最后得到点 $P=(x_2,x_2+X_2)$。下面的引理可以判别哪一个是 x_2 的正确解。

引理 2　设 E_{B,d_1,d_2} 的群的阶为 $2r$ 且 $E_{B,d_1,d_2}(F_{2^d})=G\times E^{[2]}$,其中 r 和 d 为奇数。点 $P=(x,y)$ 属于子群 G 当且仅当 $\mathrm{Tr}(d_1^2+d_2+d_1(d_1^2+d_1+d_2)(x+y)/(xy+d_1(x+y)))=0$.

证明　二元 Edwards 曲线 $E_{B,d_1,d_2}: d_1(x+y)+d_2(x^2+y^2)=xy+xy(x+y)+x^2y^2$ 双有理等价于 Weierstrass 曲线[4] $E: v^2+uv=u^3+(d_1^2+d_2)u^2+d_1^4(d_1^4+d_1^2+d_2^2)$。

文献[5]已经指出,在特征 2 的域中 Weierstrass 曲线上的一个点 $Q=(u,v)$ 在属于子群 G 当且仅当存在 $\lambda\in F_{2^d}$ 使得 $\lambda^2+\lambda=a+u$,即迹函数 $\mathrm{Tr}(a+u)=0$,其中 $a=d_1^2+d_2$, $u=d_1(d_1^2+d_1+d_2)(x+y)/(xy+d_1(x+y))$。

2.2　半分算法

令 $Q=(x_4,y_4)\in G$, $P=(x_2,y_2)$, $Q=2P$, $X_2=x_2+y_2$, $X_4=x_4+y_4$, $M=1/(d_1/d_2+(1+d_1/d_2)X_4+X_4^2)$。

算法 1. $d_1\neq d_2$ 时的半分算法。

输入:(x_4,y_4)　输出:(x_2,y_2)

1) $c_0\leftarrow d_2+d_1(((d_1/d_2)M+MX_4)+(d_1+d_2)(((d_1/d_2)M+MX_4)^2$;

2) $t_1\leftarrow\sum_{i=0}^{(d-3)/2}c_0^{2^{(2i+1)}}$;

3) $a_0\leftarrow(d_1/d_2)[1+(1+d_1/d_2)(M+MX_4)]$;

4) $t\leftarrow a_0t_1$;

5) $b_0\leftarrow d_2+d_2/(1+t)$;

6) 若 $\mathrm{Tr}(b_0)=0$,则 $X_2\leftarrow\sqrt{t}$,反之,$X_2\leftarrow\sqrt{t+a_0}$;

7) $f_0\leftarrow(y_4+1)(d_1+X_2^2+X_2^4d_2/d_1)+d_1+d_2X_2^2$;

8) $x'_2\leftarrow\sum_{i=0}^{(d-3)/2}f_0^{2^{(2i+1)}}$;

9) $e_0\leftarrow\sqrt{x'_2}$;

10) $g_0\leftarrow d_1^2+d_2+d_1(d_1^2+d_1+d_2)X_2/(x'_2+(e_0+d_1)X_2)$;

11) 若 $\mathrm{Tr}(g_0)=0$,则返回 $P=(e_0,e_0+X_2)$,反之返回 $P=(\sqrt{x'_2+1},\sqrt{x'_2+1}+X_2)$。

上述的半分算法需要 3I + 5M + 4S + 2H + 2SR + 2T 的计算量(这里忽略由曲线参数产生的乘法)。如果我们采用正规基表示,那么平方、平方根、半迹函数和迹函数的计算都是可忽略的,这时总的计算量就是 3I + 5M。这里的 M 表示域乘法,S 为平方,I 为逆,SR 为平方根,H 为半迹函数,T 为迹函数。

如果当 $d_1=d_2$ 时,二元 Edwards 曲线的半分算法可以用上面的算法计算,那么将会很有效。但不幸的是,当 $d_1=d_2$ 时半分算法效率反而更低。

3　半分算法(当 $d_1=d_2$ 时)

非奇异曲线 E 定义如下[5]:

$v^2+uv=u^3+a_2u^2+a_6$, $a_2,a_6\in F_{2^n}$, $a_6\neq0$.

我们与文献[5]一样用 T_{2^k} 表示一个阶为 2^k 的点。当曲线有最小 2 - 挠点时, $E(F_{2^n})=G\times E[2^k]$,其中 $k=1$, G 为奇数阶的群。而且有下面的等价形式[3]:

$$T_4\in E(F_{2^n})\Leftrightarrow\exists\lambda\in F_{2^n}:\lambda^2+\lambda=a_2.$$

令 F 表示域 F_{2^n} 上的线性变换 $F(\lambda)=\lambda^2+\lambda$,文献[5]有结论:$E$ 有最小 2 挠点 $\Leftrightarrow a_2\notin\mathrm{Im}(F)$。

定理 1　当 $d_1=d_2$ 时,二元 Edwards 曲线没有最小 2 挠点。

证明　当 $d_1=d_2$ 时,二元 Edwards 曲线简化为:

$$E_{B,d_1,d_2}: d_1(x+x^2+y+y^2)=(x+x^2)(y+y^2).$$

该曲线双有理等价于 Weierstrass 曲线 $E: v^2+uv=u^3+(d_1^2+d_1)u^2+d_1^8=u^3+a_2u^2+a_6$。因此,有等式 $a_2=d_1^2+d_1$ 成立。这时一定存在 $\lambda=d_1\in F_{2^n}$ 使得 $a_2=d_1^2+d_1=\lambda^2+\lambda$,即 $a_2\in\mathrm{Im}(F)$。因而当 $d_1=d_2$ 时,二元 Edwards 曲线没有最小 2

挠点。

King 和 Rubin[7] 进一步推广了 Knudsen[5] 的半分算法,使得半分算法能适合只有最小 4 挠点的群的情况。

令 $Q=(x_4,y_4)\in G$, $P=(x_2,y_2)$, $Q=2P$, $X_2=x_2+y_2$, $X_4=x_4+y_4$, $T=X_2^2$。从方程(2)可以得出 $T^2+T=d_1+d_1/(X_4+1)$。我们断定 $X_4+1\neq 0$,因为若 $X_4+1=0$,从方程(2)可以推出 $d_1=0$,这与二元 Edwards 曲线的定义矛盾。

我们可以利用前面的半分算法得到 X_2 等于 $X_4/2$ 或 $X_4/2+T_2$。但是现在我们还无法判别这两个解中哪一个是正确的解。我们可以利用与文献[7]一样的方法来判别。最后当我们得到正确的解 X_2 之后可以用一个半迹函数和引理 2 得到最终的正确的解。

4 有效性分析并应用于标量乘计算上

二元 Edwards 曲线当 $d_1=d_2$ 时的半分算法需要两次判别算法才能得到正确的解,这个过程计算耗费很多,所以并不实用。因此,我们仅分析 $d_1\neq d_2$ 的情况。

如果我们采用正规基表示,一个平方运算只是简单的向量移位。平方根计算也是一样的,只是移位的方向与平方计算相反。由于迹函数和半迹函数是平方幂次运算的和,所以也可以很简单地计算。

在半分算法里,我们需要判别正确的解,这个过程花费 1I+3M+2S+1H+1T+1SR(忽略方程参数的乘法)。但是,我们如果采用 ω - 坐标来计算标量乘,那么就只需要在标量乘计算的最后判别正确的解就可以,从而可以节省很多计算量。

用文献[4]的差分加法可以简化半分算法。令 $\omega_i=X_i$,我们只需计算半分算法的第 1 ~ 6 步。

把半分 - 点加方法用在差分加法上,我们可以计算任何标量乘 mP。最后,令 $E=\omega_1+\omega_2$, $F=\omega_1\omega_2$, $G=\omega_2^2+\omega_2$ 可以得到:

$$x_2^2+x_2=\frac{\omega_3(d_1+F(E+1)+F^2d_2/d_1)+d_1E+(y_1^2+y_1)G}{\omega_1^2+\omega_1}.$$

给定 (x_1,y_1) 和 (x_3,y_3),除了 $\omega_1^2+\omega_1=0$ 简单情况[4]外,上述公式总存在一个解 (x_2,y_2)。计算一个半迹函数就可以得到两个解 x_2 和 x_2+1,因此可以得到两个点 $mP=(x_2,y_2)$ 和 $mP=(x_2+1,y_2+1)$。

最后有两个解,如果用倍加 - 点加方法计算将比较难判别哪一个是正确的解。用半分 - 点加方法计算则可以很容易地用引理 2 判别出正确的解。

5 结 论

本文提出并分析了二元 Edwards 曲线的半分算法。并把该半分算法用于标量乘计算上,不过我们的半分算法并没有比倍加算法快。即使我们采用 ω - 坐标来计算标量乘,半分 - 点加算法仍然比倍加 - 点加算法稍慢。

参考文献(References)

[1] Edwards H M. A normal form for elliptic curves[J]. Bulletin of the American Mathematical Society, 2007,44: 393 - 422.

[2] Bernstein D J, Lange T. Faster addition and doubling on elliptic curves[C]// Proc of ASIACRYPT 2007, LNCS 4833, 2007: 29 - 50.

[3] Bernstein D J, Birkner P, Joye M, et al. Twisted edwards curves [C]// Proc of AFRICACRYPT 2008, LNCS 5023, 2008: 389 - 405.

[4] Bernstein D J, Lange T, Rezaeian Farashahi R. Binary edwards curves [C]// Proc of CHES 2008, LNCS 5154, 2008: 244 - 265.

[5] Knudsen E. Elliptic scalar multiplication using point halving [C]// Proc of ASIACRYPT 1999, LNCS 1716, 1999: 135 - 149.

[6] Schroeppel R. Elliptic curve point halving wins big [C]// Proc of 2nd Midwest Arithmetical Geometry in Cryptography Workshop, 2000.

[7] King B, Rubin B. Improvements to the point halving algorithm [C]// Proc of ACISP 2004, LNCS 3108, 2004: 262 - 276.

[8] Avanzi R, Ciet M, Sica F. Faster scalar multiplication on koblitz curves combining point halving with the frobenius endomorphism [C]// Proc of PKC 2004, LNCS 2947, 2004: 28 - 40.

[9] Birkner P. Efficient divisor class halving on genus two curves [C]// Proc of SAC 2006, LNCS 4356, 2006: 317 - 326.

[10] Birkner P, Theriault N. Faster halvings in tenus 2 [C]// Proc of SAC 2008, LNCS 5381, 2008: 1 - 17.

[11] Fong K, Hankerson D, Lopez J, et al. Field inversion and point halving revisited [J]. IEEE Transactions on Computers, 2003,53: 1047 - 1059.

[12] Kitamura I, Katagi M, Takagi T. A complete divisor class halving algorithm for hyperelliptic curve cryptosystems of genus two [C]// Proc of ACISP 2005, LNCS 3574, 2005: 146 - 157.

[13] Avanzi R, Cohen H, Doche C, et al. Handbook of elliptic and hyperelliptic curve cryptography [M]. CRC Press, Boca Raton, 2005.