

へ

ア
リ
ン
グ
演
算
の
高
速
化
Signed
Miller
Al-
go-
rithm
第
4
章
で
述
べ
た
Miller
Al-
go-
rithm
で
は
部
分
群
の
位
数
 n
を
2
進
展
開
し
て
い
た.
Signed
Miller
Al-
go-
rithm
は
符
号
付
き
2
進
展
開
を
用
い
る
手
法
で
あ
る.
次
に
そ
の
ア
ル
ゴ
リ
ズ

Input: $n, P = (x_P, y_P) \in E(F_q)[n], Q = (x_Q, y_Q) \in E(F_{q^k})$

Output: $f \in F_{q^k}$

```

1:  $Q' \in_R E(F_{q^k})$ 
2:  $S = Q + Q' \in E(F_{q^k})$ 
3:  $V \leftarrow P, f \leftarrow 1, f_{-1} = \frac{1}{x_Q - x_P}$ 
4:  $n = \sum_{i=0}^{l-1} n_i 2^i, n_i \in \{-1, 0, 1\}, n_0 = 1$ 
5: for  $j \leftarrow l-1$  down to 0
6:    $f \leftarrow f^2 \cdot \frac{g_{V,V}(S)g_{2V}(Q')}{g_{2V}(S)g_{V,V}(Q')}$ 
7:    $V \leftarrow 2V$ 
8:   if  $n_j = 1$  then
9:      $f \leftarrow f \cdot \frac{g_{V,P}(S)g_{V+P}(Q')}{g_{V+P}(S)g_{V,P}(Q')}$ 
10:     $V \leftarrow V + P$ 
11:   if  $n_j = -1$  then
12:      $f \leftarrow f \cdot f_{-1} \cdot \frac{g_{V,P}(S)g_{V-P}(Q')}{g_{V-P}(S)g_{V,P}(Q')}$ 
13:     $V \leftarrow V - P$ 
14: return  $f$ 

```

Signed

Miller

Al-

go-

rithm

このように符号付きで展開する方法は後述のアルゴリズムでも同様に用いることができる。

高
速
化
手
法
su-
per-
sin-
gu-
lar
curve
に
お
け
る
Re-
duced
Tate
ペ
ア
リ
ン
グ
の
高
速
化
手
法
が
Bar-
reto
ら
に
よ
っ
て
い
く
つ
か
提
案
さ
れ
た
[?].
そ
れ
を
次
に
列
挙
す
る.
部
分
体
の
要
素
に
よ
る
乗
算
埋
め
込
み
次
数
 k
の
因
子