# 亏格为3的超椭圆曲线除子加法的并行算法

郝艳华　范欣欣　王育民
（西安电子科技大学 ISN 国家重点实验室　西安 710071）

**摘　要**　本文给出了求超椭圆曲线除子加法并行算法的一个易于实现的一般性方法，使用该方法得到的并行算法的并行轮数是最小的。将该方法应用于亏格为3的超椭圆曲线除子加法运算中，得到分别使用9和7个乘法处理器，可在15轮运算中实现除子加法和倍点运算的一个并行算法。

**关键词**　超椭圆曲线密码体制，亏格为3的超椭圆曲线，除子，并行算法

## Parallelizing Explicit Formula in Genus 3 Hyperelliptic Curves

HAO Yan-Hua　FAN Xin-Xin　WANG Yu-Min
(Nation Key Laboratory on ISN, Xidian University, Xi'an710071)

**Abstract**　A general methodology for obtaining parallel algorithm of divisor arithmetic in hyperelliptic curve, which is easy to perform, is developed. The algorithm is optimal in the number of parallel rounds. Applying this methodology, we derive the parallel version of the explicit formula for divisor arithmetic in genus 3 hyperelliptic curve. It is shown that with 9 multipliers and 7 multipliers respectively, the divisor addition and doubling can be carried out in at least 15 parallel rounds.

**Keywords**　Hyperelliptic curve cryptosystem, Genus 3 hyperelliptic curve, Divisor, Parallel algorithm

自1988年Koblitz首次提出超椭圆曲线密码体制(HECC)[1]以来，人们普遍认为，由于运算效率较低，与椭圆曲线密码体制(ECC)相比，超椭圆曲线密码体制在实现方面没有什么优势。然而，至今仍有许多研究者没有放弃对超椭圆曲线密码体制的研究，这是因为它有许多椭圆曲线密码体制无法比拟的优点。其中较为重要的一个就是与椭圆曲线密码体制相比，超椭圆曲线密码体制所需的基域更小：要达到160比特ECC的安全性，亏格为2的HECC的基域需80比特，而亏格为3的HECC的基域则只需54比特就足够了，这使得无需进行多精度计算就可以在64比特CPU上来实现它，因此超椭圆曲线密码体制更适宜在受限系统中使用。

影响HECC投入实际应用的一个重要因素就是它的实现速度问题，这也是许多研究者研究的主要课题。目前对这个问题的解决主要是通过两种途径：第一种途径就是研究超椭圆曲线除子加法的确定性公式本身[2~5]，通过使用一些数学技巧来简化公式、合并运算的方法来提高效率。就目前所知，奇特征域上亏格为3的超椭圆曲线除子加法的最快算法是由Gonda等人给出的[6]，使用该算法除子加法需 $I+70M+113A$，而除子倍点需 $I+71M+107A$，其中 $I$、$M$ 和 $A$ 分别表示进行一次基域中元素的求逆运算、乘法运算和加法运算所需要的时间。由于基域中乘方运算和乘法运算所需时间相差不多，因此进行一次乘方运算所需的时间也记为 $M$。但是由于超椭圆曲线上Jacobian群本身结构复杂，对公式本身进行改进来达到提高效率就显得收效甚微。很多时候人们不得不考虑采用第二种途径，那就是通过研究超椭圆曲线除子加法的并行算法来提高实现速度。Mishra首先给出了一个亏格为2的超椭圆曲线除子加法的并行算法[7]，得出最好的结果是加法运算至少需要8个乘法器进行8轮运算，倍点运算至少需要11个乘法器进行8轮运算。本文将进一步改进该并行算法并利用Gonda等人[6]的确定性公式给出亏格为3的超椭圆曲线上除子运算的并行算法。

## 1　超椭圆曲线密码体制的数学基础

令 $K$ 为一有限域，$\overline{K}$ 为 $K$ 的代数闭包，定义在 $K$ 上的亏格为 $g(g\geqslant 1)$ 的超椭圆曲线 $C$ 由下式给出：

$$C: v^2+h(u)v=f(u) \tag{1.1}$$

其中 $h(u)\in K(u)$ 是一个至多 $g$ 次的多项式，$f(u)\in K(u)$ 是一个 $2g+1$ 次的首一多项式，并且没有数对 $(u,v)\in\overline{K}\times\overline{K}$ 能够同时满足方程(1.1)及方程(1.1)的两个偏微分方程 $2v+h(u)=0$ 和 $h'(u)v-f'(u)=0$。$C$ 在 $\overline{K}$ 上是不可约的。

令有限域 $K$ 的特征为奇数，构造一个变换 $\varphi: u\to u, v\to(v-h(u)/2)$，可将 $C$ 的方程变为形式 $v^2=f_1(u)$ 为的方程，其中 $f_1(u)\in K(u)$ 是一个 $2g+1$ 次的首一多项式。所以以后我们考虑奇特征域上的超椭圆曲线的时候，只需考虑形式为 $C: v^2=f(u)$ 的方程就足够了。特别地，特征为奇数的域上的亏格为3的超椭圆曲线方程可写为

$$y^2=x^7+f_6x^6+f_5x^5+\cdots+f_0 \tag{1.2}$$

其中 $f_i\in K$。假定 $K$ 的特征不为2和7，通过变换 $\gamma: x\to x+f_6/7, y\to y$，可将方程(1.2)化为

$$y^2=x^7+f_5x^5+\cdots+f_0 \tag{1.3}$$

其中 $f_i\in K$。因此对于奇特征域上亏格为3的超椭圆曲线，本文总是设定 $f_6=0$。

超椭圆曲线 $C$ 上的除子 $D$ 定义为 $C$ 上点的形式和

郝艳华　博士生，研究方向为超椭圆曲线密码体制和信息安全；范欣欣　硕士，研究方向为超椭圆曲线密码体制研究；王育民　教授，博士生导师，长期从事信息论、编码与必码学的教学和科研工作。

$D=\sum_{P\in C} m_P P, m_P \in Z$

其中只有有限个数的 $m_P$ 非零。整数 $\sum_{P\in C} m_P$ 称为 $D$ 的次数，记为 $degD$。所有除子组成的集合 $D$ 在如下定义的加法运算下构成一个加法群：

$$\sum_{P\in C} m_P P+\sum_{P\in C} n_P P=\sum_{P\in C}(m_P+n_P)P$$

所有 0 次除子组成的集合是 $D$ 的一个子群，记为 $D^0$。

令 $D_1=\sum_{P\in C} m_P P$ 和 $D_2=\sum_{P\in C} n_P P$ 是两个除子，则 $D_1$ 和 $D_2$ 的最大公因子定义为

$$\gcd(D_1,D_2)=\sum_{P\in C}\min(m_P,n_P)/P-(\sum_{P\in C}\min(m_P,n_P))\infty$$

令 $K[C]=K[u,v]/(v^2+h(u)v-f(u))$，则 $K[C]$ 的分式域 $K(C)$ 称为 $C$ 在 $K$ 上的函数域。对于多项式 $G\in K(C)$，$G$ 的除子定义为 $\mathrm{div}(G)=\sum_P ord_P(G)P$，其中 $ord_P(G)$ 是 $G$ 在 $P$ 点零化的阶。有理函数 $F=G/H$ 的除子定义为 $div(F)=\mathrm{div}(G)-\mathrm{div}(H)$，除子 $D\in D^0$ 称为是主除子。如果存在某个有理函数 $R\in K(C)$，使得 $D=\mathrm{div}(R)$。所有主除子的集合是 $D^0$ 的子群，记为 $P$。商群 $J=D^0/P$ 称为曲线 $C$ 的 Jacobian。

一个除子称为半归约的，如果它的形式表示中没有两个点是互负的。如果这样的一个除子具有 $k$ 个点(可重复)，则称这个半归约除子的权是 $k$。$k\leqslant g$ 的半归约除子称为归约除子。商群 $J$ 的每一个陪集中都恰好只有一个归约除子，因此 $J$ 实际上可以表示成超椭圆曲线 $C$ 上的全体归约除子的集合，在 $J$ 中定义归约除子的加法运算，则 $J$ 在这个加法运算下就可构成一个交换群。超椭圆曲线密码实际上就是建立在这个交换群上的。$J$ 中的元素 $D=\sum m_i P_i-(\sum m_i)\infty$(这里 $\sum m_i\leqslant g, P_i=(x_i,y_i)$)，可由 $K[x]$中的两个多项式 $a$ 和 $b$ 唯一确定，其中 $a(x)=\prod(x-x_i)^{m_i}$，且 $a$ 和 $b$ 满足：1) $\deg b<\deg a\leqslant g$；2)对所有 $m_i\neq 0$ 的 $i, b(x_i)=y_i$；3) $b^2+hb-f\equiv 0 \pmod a$。$D=\gcd(\mathrm{div}(a),\mathrm{div}(b-y))$，一般简记为 $D=[a,b]$。

## 2 确定性公式并行的一般方法

超椭圆曲线除子加法及倍点算法是由一系列基域中加法、乘法及求逆等基本运算组成的。通常情况下，该算法都包含一次求逆运算。由于一般求逆运算都比加法和乘法运算耗时得多，因此进行公式并行的时候都可以先不考虑求逆运算，而将其他运算并行以后，再将求逆运算作为单独的一轮放在合适的位置上就可以了。又由于通常基域中加法运算要比乘法或乘方运算快得多，乘法或乘方运算的运算次数是除子加法或倍点算法运行快慢的一个重要影响因素，因此在进行公式并行的时候，主要考虑基域中乘法运算的并行，而暂不考虑加法运算的并行。文[7]给出了确定性公式并行的一般方法，构造了一个有向无圈图。但是当乘法运算的次数较多时，需要构造的这个图往往会非常复杂，会给寻找各乘法运算之间的关系带来一些困难，比较容易出错。这里我们给出一个较为简单、易操作的方法，使用这个方法得到的并行算法的特点是：1)需要运行的轮数 $r$ 最少；2)在 1)满足的情况下，所需的并行运算乘法处理器 $MW$ 的个数最少；3)在 2)满足的情况下，一次需要存储的变量的最大个数 $BW$ 最少。算法中乘法运算的总数记为 $TM$。

首先，将算法中的乘法运算拆解为每两个元素相乘的形式，我们称为二元乘，并在任一个二元乘后面标明该步最早可在第几步执行。例如计算 $s=i*j*k$，其中 $*$ 为域乘运算。如果算法中 $i,j$ 和 $k$ 均为已知的参数，则可这样拆解：$t=i*j$(1)，(1)标明这一步在第一步就可完成；$s=t*k$(2)，(2)标明这一步最早可在第二步完成；$t$ 是引入的中间变量。如果算法中 $i,j$ 和 $k$ 均不是已知的参数，假设 $i$ 最早可在 $u_i$ 步生成，$j$ 最早可在 $u_j$ 步生成，而 $k$ 最早可在 $u_k$ 步生成，且 $u_i<u_j<u_k$，则上式可拆解为 $t=i*j(u_j+1)$；$s=t*k(\max(u_j+1,u_k)+1)$。其他情形可类似拆解。当然拆解的方法很多，这种拆解方法可以使得各步都能尽早完成。任两个二元乘之间有两种关系：一种是这两个二元乘之间没有任何顺序关系，可以并行进行，我们称这两个二元乘是无关的；另一种是这两个二元乘在计算上有顺序关系，一个二元乘必须在另一个二元乘完成之后才能进行，我们就说这两个二元乘是相关的。按照我们的方法拆解，后面标号相同的二元乘相互之间一定是无关的，因此是可以并行计算的；而标号不同的二元乘，则既可以是相关的，也可以是无关的。因为乘法运算的数目是有限的，拟存在某个二元乘的后面是一个最大标号 $l$。由于这个标号表示该步最早可在第 $l$ 步完成，因此如果给出足够的资源，整个算法可在 $l$ 步内并行完成。因此，$l$ 就是我们要找的并行算法的最小轮数 $r$。

找到了并行算法的最小轮数 $r$，我们需要寻找所需乘法处理器的最小个数 $MW$，使得如果使用少于 $MW$ 个乘法处理器，那么得到的并行算法的轮数将会大于 $r$，而使用多于 $MW$ 个乘法处理器，所得到的并行算法的轮数仍将等于 $r$。一个最直接的想法就是 $MW=\lceil TM/r\rceil$，但是一般情况下，这个式子都是不成立的。这个式子只适用于那些乘法运算分布非常均匀的情况，而这种情况是非常少的。$MW$ 的值与具体算法中乘法运算的分布有很大关系，因此很难使用一个统一的公式来表示这个值。本文中我们采取先给出一个估计的最小值，然后用边测试边递增这个最小值的方法。比如，如果这个最小值我们给出的是 6，那么我们就尝试使用 6 个乘法处理器来并行这个算法，看看是否能够在第 $r$ 轮完成。如果在第 $r$ 轮完成了，说明 $MW=6$，否则就继续使用 7 个乘法处理器来并行算法，直到找到 $MW$ 的值为止。因此，较准确地估计最小值，可使我们少进行无谓的测试，简化我们的设计过程。

令 $v=\lceil TM/r\rceil$。对于一般算法，我们知道都有 $MW\geqslant v$。但是，如果我们以 $v$ 作为最小值来测试的话，在找到 $MW$ 值之前可能需要进行较多的测试，因此我们考虑是不是能找到更为精确一些的值。我们将后面标号相同的二元乘放在一起来观察该算法中乘法运算分布情况，寻找是否存在某一个标号 $i$，使得标号小于或等于这个标号的所有二元乘的个数小于 $iv$，这个个数记为 $TM_i$。令 $z_i=\lceil(TW-TM_i)/(r-i)\rceil$，由于二元乘后面的标号表示的是该二元乘最早可进行的轮数，因此标号大于 $i$ 的二元乘都不可能在第 $i$ 轮及以前的各轮中完成，所以剩余 $TM-TM_i$ 个二元运算都必须在 $r-i$ 轮完成，就有 $MW\geqslant z_i$。找出所有的这样的 $z_i$ 值，取其中最大的那一个与 $v$ 做比较，取较大的一个作为我们测试的最小值 $MW_{\min}$。

有了最小值 $MW_{\min}$之后，我们就可以开始测试了。测试的方法是这样的：我们把后面标号最大的二元乘全部写在第一组里。如果这样的二元乘法的个数小于 $MW_{\min}$，就考虑标号次大的二元乘里有没有与写在第一组里的二元乘无关的。如果有，也写在第一组里。如果这样的元考虑完以后，第一组二元乘的个数仍然小于 $MW_{\min}$，那就再考虑标号再次大的。总之，一定按照标号从大到小的顺序一层层考虑，直到第一组

个数正好等于$MW_{min}$，或是第一组个数虽不等于$MW_{min}$，但已经没有其它元可与第一组中各元不相关为止。标号为$r$的二元乘个数不可能大于$MW_{min}$，否则，一定有$z_r > MW_{min}$，这与$MW_{min}$的取法相矛盾。第一组选取完以后再选第二组，首先考虑没有选过的标号最大的二元乘，将最大可能的不相关的二元乘都写进来，后面的都类似，最后看看是否能在$r$轮完成。最后通过测试找到$MW$值，将找到这个值的测试算法倒过来写，即将第$r$组写为第1轮，第$r-1$组写为第2轮，……，第1组写为第$r$轮。

然后将求逆轮加到合适的地方，最后一步就是将加法运算添加进去。因为不考虑加法运算的并行，所以任何相邻的轮数之间可以有多个串行的加法运算，原则就是要使用最少的变量，任何新的加法变量的生成最好挨近第一次引用它的乘法运算。

## 3 亏格为3的超椭圆曲线除子加法的并行算法

我们将上述方法应用到文[6]给出的亏格为3的超椭圆曲线除子加法算法中，得到了亏格为3的超椭圆曲线除子加法的并行算法。文[6]中加法运算需要$I+70M+113A$，而倍点运算需要$I+71M+107A$。在进行运算$A=B+C+D, E=F(A-C)$的时候(其中，$B,C,D$和$F$均是域元素)，文[6]均按照3个加法、一个乘法的运算量。其实，改变加法的顺序，比如$G=B+D, A=C+G, E=FG$，则只需2个加法、一个乘法就够了，所以做并行的时候，我们按照加法需$I+70M+112A$，倍点需$I+71M+106A$来计算。

首先我们将加法和倍点算法中的乘法运算拆解成二元乘形式并在后面标号，将后面标号相同的二元乘整理，得到表1和表2。

表1 加法运算

| 标号数 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 二元乘的个数 | 6 | 6 | 7 | 6 | 3 | 2 | 2 | 3 | 11 | 8 | 4 | 7 | 4 | 1 |

表2 倍点运算

| 标号数 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 二元乘的个数 | 11 | 9 | 6 | 6 | 3 | 2 | 2 | 3 | 11 | 4 | 4 | 7 | 2 | 1 |

从这两个表我们首先可以得出，对于加法算法和倍点算法来说，$r$都是14。又由于这两个算法都包含一个求逆运算，把求逆运算单独作为1轮，因此这两个算法的并行算法都是至少15轮。对于加法算法，$v=\lceil 70/14 \rceil = 5$。由于$TM_7 = 6+6+7+6+3+2+2 = 32 < 5*7 = 35$，因此$z_7 = \lceil (70-32)/(14-7) \rceil = 6$；$TM_8 = 6+6+7+6+3+2+2+3 = 35 < 5*8 = 40$，所以$z_8 = \lceil (70-35)/(14-8) \rceil = 6$，因此$MW_{min} = 6$；对于倍点算法，同样方法可以计算出$MW_{min} = 6$。通过测试发现，使用6个乘法处理器无法在15轮中完成加法和倍点运算。通过验证，加法算法中至少需要9个乘法处理器，倍点算法中只需要7个就够了。除子加法算法和倍点算法的并行算法将在后面附录中详细给出。

**结论** 本文给出了求超椭圆曲线除子加法和倍点并行算法的一个易于实现的一般性方法，利用这个方法给出了亏格为3的超椭圆曲线除子加法的一个并行算法。结果表明，加法运算使用9个乘法处理器至少需要进行15轮运算(其中包含一个求逆轮)，倍点运算使用7个乘法处理器也至少需要进行15轮运算(其中包含一个求逆轮)。由于超椭圆曲线密码具有其他公钥密码所无法比拟的优势，因此研究它的性能以帮助它早日走向实用，是一个非常有价值的方向。

## 参 考 文 献


1 Koblitz N. A Family of Jacobians Suitable for Discrete Log Cryptosystems. In: Goldw-assers, ed. Advances in Cryptology-Crypto'88. Berlin: Spinger-Verlag, LNCS 403, 1998. 94～99

2 Cantor D C, Computing in the Jacobian of hyperelliptic curve. Math Comp, 1987, 48(177): 95～101

3 Harley R. adding. text, doubling. c, http://cristal. inria. fr/~harley/hyper/, 2000

4 Kuroki J, Gonda M, Matsuo K, et al. Fast genus three hyperelliptic curve cryptosystems. In: Proc. of SCIS2002, 2002. 503～507

5 Pelze J, Wollinger T, Guajardo J. In: Hyperelliptic curve cryptosystems: Closing the performance gap to elliptic curves (update), Cryptology ePrint Archive: [Report 2003/026]. 2003

6 Gonda M, Matsuo K, Aoki K. Improvements of addition algorithm on g-enus 3 hyperelliptic curves and their implementations. In: The 2004 Symposium on Cryptograp-hy and Information Security, Sendai, Japan, 2004

7 Mishra P K, Sarkar P. Parallelizing Explicit Formula for Arithmetic in the Jacobian of Hyp-erelliptic Curves. In: Proceedings of Asiacrypt, LNCS 2894, 2003. 93～110


**附录**：亏格为3的超椭圆曲线除子加法和倍点算法的并行算法

1. 加法算法

输入：亏格为3的超椭圆曲线$C: y^2 = x^7 + f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0$；

归约除子$D_1(U_1, V_1)$和$D_2 = (U_2, V_2)$，

$U_1 = x^3 + u_{12}x^2 + u_{11}x + u_{10}$，$V_1 = v_{12}x^2 + v_{11}x + v_{10}$，

$U_2 = x^3 + u_{22}x^2 + u_{21}x + u_{20}$，$V_2 = v_{22}x^2 + v_{21}x + v_{20}$；

输出：$D_3 = (U_3, V_3) = D_1 + D_2$，$U_3 = x^3 + u_{32}x^2 + u_{31}x + u_{30}$，

$V_3 = v_{32}x^2 + v_{31}x + v_{30}$；

初始变量：$u_{12}, u_{11}, u_{10}, v_{12}, v_{11}, v_{10}, u_{22}, u_{21}, u_{20}, v_{22}, v_{21}, v_{20}$。

第一轮

$AM01.\ p1 = u_{11}u_{20}$；$AM02.\ p_2 = u_{10}u_{21}$；

$AM03.\ p_3 = u_{12}u_{20}$；$AM04.\ p_4 = u_{10}u_{22}$；

$AM05.\ p_5 = u_{12}u_{21}$；$AM06.\ p_6 = u_{11}u_{22}$.

变量：$p_1, p_2, p_3, p_4, p_5, p_6$.

$AA01.\ t_1 = p_1 - p_2$；$AA02.\ t_2 = p_3 - p_4$；

$AA03.\ t_3 = u_{20} - u_{10}$；$AA04.\ t_4 = u_{21} - u_{11}$；

$AA05.\ t_5 = u_{22} - u_{12}$；$AA06.\ p_7 = p_5 - p_6$；

$AA07.\ t_8 = p_7 + t_3$.

变量：$t_1, t_2, t_3, t_4, t_5, t_8$.

第二轮

$AM07.\ p_9 = t_1t_5$；$AM08.\ p_{10} = t_2t_5$；

$AM09.\ p_{16} = t_5t_8$；$AM10.\ t_6 = t_4^2$；

$AM11.\ t_7 = t_3t_4$.

变量：$p_9, p_{10}, p_{16}, t_1, t_2, t_3, t_6, t_7, t_8$.

$AA08.\ i_2 = p_{16} - t_6$；$AA09.\ t_{10} = p_{10} - t_7$；

$AA10.\ t_{12}v_{12} - v_{22}$.

变量：$i_2$，$t_{10}$，$t_{13}$，$p_9$，$t_1$，$t2$，$t_3$，$t_6$，$t_7$，$t_8$.

第三轮

$AM12.\ p_8=t_3^2$；$AM13.\ p_{17}=u_{22}i_2$；

$AM14.\ p_{18}=u_{21}i_2$；$AM15.\ p_{19}=u_{22}t_{10}$；$AM16.\ t_{16}=t_{13}i_2$.

变量：$p_8$，$p_9$，$p_{17}$，$p_{18}$，$p_{19}$，$i_2$，$t_1$，$t_2$，$t_6$，$t_7$，$t_8$，$t_{10}$，$t_{13}$，$t_{16}$.

$AA11.\ i_1=p_{17}-t_{10}$；$AA12.\ t_{12}=v_{11}-v_{21}$；

$AA13.\ p_{21}=t_{12}+t_{13}$；$AA14.\ p_{22}=i_1+i_2$；

$AA15.\ t_{11}=v_{10}-v_{20}$；$AA16.\ t_p=p_8-p_9$；

$AA17.\ p_{20}=p_{19}+t_9$；$AA18.\ i_0=p_{18}-p_{20}$；

$AA19.\ p_{12}=t_{10}-t_7$；$AA20.\ p_{31}=t_{11}+t_{13}$；

$AA21.\ p_{32}=i_0+i_2$；$AA22.\ p_{41}=t_{11}+t_{12}$；

$AA23.\ p_{42}=i_0+i_1$

变量：$i_0$，$i_1$，$p_{12}$，$p_{21}$，$p_{22}$，$p_{31}$，$p_{32}$，$p_{41}$，$p_{42}$，$t_1$，$t_2$，$t_6$，$t_8$，$t_9$，$t_{11}$，$t_{12}$，$t_{16}$.

第四轮

$AM17.\ t_{14}=t_{12}i_1$；$AM18.\ t_{17}=u_{22}t_{16}$；

$AM19.\ p_{23}=p_{21}p_{22}$；$AM20.\ t_{15}=t_{11}i_0$；$AM21.\ p_{14}=t_1t_6$.

变量：$p_{12}$，$p_{14}$，$p_{23}$，$p_{31}$，$p_{32}$，$p_{41}$，$p_{42}$，$t_2$，$t_8$，$t_9$，$t_{14}$，$t_{15}$，$t_{16}$，$t_{17}$.

$AA24.\ p_{24}=t_{14}+t_{17}$；$AA25.\ p_{25}=p_{24}-p_{23}$；

$AA26.\ t_{18}=p_{25}+t_{16}$；$AA27.\ t_{19}=u_{20}+u_{22}$；

$AA28.\ p_{26}=t_{19}+u_{21}$；$AA29.\ p_{27}=t_{19}-u_{21}$；

$AA30.\ p_{28}=t_{16}+t_{18}$；$AA31.\ p_{45}=t_{14}+t_{15}$.

变量：$p_{12}$，$p_{14}$，$p_{25}$，$p_{26}$，$p_{27}$，$p_{28}$，$p_{31}$，$p_{32}$，$p_{41}$，$p_{42}$，$p_{45}$，$t_2$，$t_8$，$t_9$，$t_{14}$，$t_{16}$，$t_{17}$，$t_{18}$.

第五轮

$AM22.\ p_{11}=t_8t_9$；$AM23.\ p_{13}=t_2p_{12}$；

$AM24.\ t_{20}=p_{25}p_{26}$；$AM25.\ t_{21}=p_{27}p_{28}$；

$AM26.\ p_{29}=u_{20}t_{18}$. $AM27.\ p_{33}=p_{31}p_{32}$.

变量：$p_{11}$，$p_{13}$，$p_{14}$，$p_{29}$，$p_{33}$，$p_{41}$，$p_{42}$，$p_{45}$，$t_{14}$，$t_{16}$，$t_{17}$，$t_{20}$，$t_{21}$.

$AA32.\ p_{15}=p_{11}+p_{13}$；$AA33.\ r=p_{14}+p_{15}$；

$AA34.\ p_{30}=p_{29}+t_{15}$；$AA35.\ s'_0=-p_{30}$；

$AA36.\ p_{34}=t_{20}+t_{21}$；$AA37.\ p_{35}=p_{34}/2$；

$AA38.\ p_{36}=t_{14}+p_{33}$；$AA39.\ p_{37}=S'_0+p_{36}$；

$AA40.\ p_{38}=p_{35}+p_{37}$；$AA41.\ s'_2=t_{16}-p_{38}$；

$AA42.\ p_{39}=t_{21}-t_{20}$.

变量：$r$，$s'_0$，$s'_2$，$p_{39}$，$p_{41}$，$p_{45}$，$t_{17}$.

第六轮

$AM28.\ p_{47}=rs'_2$.

变量：$s'_0$，$s'_2$，$r$，$p_{39}$，$p_{41}$，$p_{42}$，$p_{45}$，$p_{47}$，$t_{17}$.

第七轮

$AI.\ t_{22}=p_{47}^{-1}$.

变量：$t_{22}$，$s'_0$，$s'_2$，$r$，$p_{39}$，$p_{41}$，$p_{42}$，$p_{45}$，$t_{17}$.

第八轮

$AM29.\ t_{23}=rt_{22}$；$AM30.\ p_{43}=p_{41}p_{42}$.

变量：$t_{23}$，$t_{22}$，$s'_0$，$s'_2$，$p_{39}$，$p_{43}$，$p_{45}$，$t_{17}$.

$AA43.\ p_{44}=p_{43}+t_{17}$；$AA44.\ p_{46}=p_{45}-p_{44}$；

$AA45.\ p_{40}=p_{39}/2$ $AA46.\ s'_1=p_{40}+p_{46}$.

变量：$s'_0$，$s'_1$，$s'_2$，$r$，$t_{22}$，$t_{23}$.

第九轮

$AM31.\ \omega_i=rt_{23}$；$AM32.\ s_0=t_{23}s'_0$；

$AM33.\ s_1=t_{23}s'_1$；$AM34.\ p_{48}=s'^2_2$.

变量：$\omega_i$，$s_0$，$s_1$，$p_{48}$.

$AA47.\ z_4=u_{12}+s_1$；$AA48.\ p_{58}=z_4+s_1$；

$AA49.\ u_{t3}=p_{58}-u_{22}$；$AA50.\ p_{67}=2v_{12}$；

$AA51.\ p_{68}=p_{67}-\omega_i$；$AA52.\ t_{34}=u_{t3}-z_4$；

$AA53.\ p_{51}=s_0-s_1$；$AA54.\ t_{24}=s_0+s_1$.

变量：$\omega_i$，$s_0$，$s_1$，$u_{t3}$，$z_4$，$p_{48}$，$p_{51}$，$p_{68}$，$t_{22}$，$t_{24}$，$t_{34}$.

第十轮

$AM35.\ t_{28}=u_{12}s_1$；$AM36.\ p_{59}=s_1z_4$；

$AM37.\ p_{60}=u_{22}u_{t3}$；$AM38.\ p_{76}=s_1v_{12}$；

$AM39.\ p_{79}=w_iu_{12}$；$AM40.\ p_{83}=u_{20}u_{t3}$；

$AM41.\ p_{99}=t_{34}u_{t3}$；$AM42.\ w=t_{22}p_{48}$；$AM43.\ p_{69}=\omega_ip_{68}$.

变量：$\omega_i$，$s_0$，$s_1$，$w$，$z_4u_{t3}$，$p_{51}$，$p_{59}$，$p_{60}$，$p_{69}$，$p_{76}$，$p_{79}$，$p_{83}$，$p_{99}$，$t_{24}$，$t_{28}$，$t_{34}$.

$AA55.\ p_{57}=u_{11}+s_0$；$AA56.\ z_3=p_{57}+t_{28}$；

$AA57;\ p_{63}=u_{21}+u_{22}$；$AA58.\ p_{61}=s_0-u_{21}$；

$AA59.\ p_{62}=p_{61}+z_3$；$AA60.\ t_{30}=p_{59}-p_{60}$；

$AA61.\ u_{t2}=p_{62}+t_{30}$；$AA62.\ p_{64}=u_{t2}+u_{t3}$；

$AA63.\ p_{65}=z_3+z_4$；$AA64.\ p_{100}=p_{99}+z_3$；

$AA65.\ p_{101}=p_{100}-u_{t2}$；$AA66.\ t_{25}=u_{10}+u_{12}$；

$AA67.\ p_{49}=t_{25}+u_{11}$；$AA68.\ p_{50}=t_{25}-u_{11}$；

$AA69.\ p_{77}=p_{76}+v_{11}$；$AA70.\ p_{78}=2p_{77}$；

$AA71.\ p_{80}=p_{78}+p_{79}$.

变量：$z_3$，$\omega_i$，$w$，$s_0$，$s_1$，$u_{t2}$，$u_{t3}$，$p_{49}$，$p_{50}$，$p_{51}$，$p_{63}$，$p_{64}$，$p_{65}$，$p_{69}$，$p_{80}$，$p_{83}$，$p_{101}$，$t_{24}$，$t_{28}$，$t_{30}$，$t_{34}$.

第十一轮

$AM44.\ t_{29}=s_0z_3$；$AM45.\ t_{31}=p_{63}p_{64}$；

$AM46.\ t_{32}=u_{21}u_{t2}$；$AM47.\ p_{66}=t_{24}p_{65}$；

$AM48.\ p_{95}=t_{34}u_{t2}$；$AM49.\ v_{t3}=wp_{101}$；

$AM50.\ t_{26}=t_{24}p_{49}$；$AM51.\ t_{27}=p_{50}p_{51}$；$AM52.\ z_0=u_{10}s_0$.

变量：$z_0$，$\omega_i$，$s_1$，$w$，$u_{t2}$，$u_{t3}$，$v_{t3}$，$p_{66}$，$p_{69}$，$p_{80}$，$p_{83}$，$p_{95}$，$t_{26}$，$t_{27}$，$t_{28}$，$t_{29}$，$t_{30}$，$t_{31}$，$t_{32}$，$t_{33}$，$t_{34}$.

$AA72.\ p_{70}=t_{30}+u_{20}$；$AA73.\ p_{71}=p_{70}+t_{31}$；

$AA74.\ t_{33}=t_{29}-t_{32}$；$AA75.\ p_{72}=p_{71}+t_{33}$；

$AA76.\ p_{52}=t_{26}-t_{27}$；$AA77.\ p_{53}=p_{52}/2$；

$AA78.\ z_1=p_{53}-t_{28}$；$AA79.\ p_{54}=t_{26}+t_{27}$；

$AA80.\ p_{55}=p_{54}/2$；$AA81.\ p_{56}=p_{55}+z_0$；

$AA82.\ z_2=p_{56}+u_{10}$；$AA83.\ p_{73}=z_2+p_{69}$；

$AA84.\ p_{74}=p_{73}+p_{66}$；$AA85.\ u_{t1}=p_{74}-p_{72}$；

$AA86.\ p_{96}=p_{95}+z_2$；$AA87.\ p_{97}=p_{96}-u_{t1}$；

变量：$z_0$，$z_1$，$z_2$，$\omega_i$，$w$，$s_1$，$u_{t1}$，$u_{t2}$，$u_{t3}$，$v_{t3}$，$p_{80}$，$p_{83}$，$p_{97}$，$t_{33}$，$t_{34}$.

第十二轮

$AM53.\ p_{82}=u_{22}u_{t1}$；$AM54.\ p_{91}=t_{34}u_{t1}$；

$AM55.\ p_{58}=wp_{97}$；$AM56.\ p_{102}=v_{t3}^2$；

$AM57.\ p_{75}=s_1z_2$；$AM58.\ p_{81}=\omega_ip_{80}$.

变量：$z_0$，$z_1$，$w$，$u_{t1}$，$u_{t2}$，$u_{t3}$，$v_{t3}$，$p_{75}$，$p_{81}$，$p_{82}$，$p_{83}$，$p_{91}$，$p_{98}$，$p_{102}$，$t_{33}$，$t_{34}$.

$AA88.\ p_{92}=p_{91}+z_1$；$AA89.\ p_{84}=p_{82}+p_{83}$；

$AA90.\ p_{85}=z_1+t_{33}$；$AA91.\ p_{86}=p_{75}+p_{85}$；

$AA92.\ p_{87}=p_{81}+p_{86}$；$AA93.\ u_{t0}=p_{87}-p_{84}$；

$AA94.\ p_{92}-u_{t0}$；$AA95.\ p_{103}=p_{102}+u_{t3}$；

$AA96.\ u_{32}=-p_{103}$；$AA97.\ t_{35}=2v_{t3}$；$AA98.\ v_{t2}=p_{98}+v_{12}$.

变量：$z_0$，$w$，$u_{t0}$，$u_{t1}$，$u_{t2}$，$u_{t3}$，$v_{t2}$，$v_{t3}$，$p_{93}$，$t_{34}$，$t_{35}$，$u_{32}$.

第十三轮

$AM59.\ p_{94}=wp_{93}$；$AM60.\ p_{104}=u_{32}u_{t3}$；

$AM61.\ p_{105}=t_{35}v_{t2}$.

变量：$z_0, w, u_{r0}, u_{t1}, u_{t2}, u_{t3}, v_{t2}, v_{t3}, p_{94}, p_{104}, p_{105}, t_{34}, t_{35}, u_{32}$.

$AA99.\ v_{t1}=p_{94}+v_{11}$；$AA100.\ p_{106}=u_{t2}+p_{104}$；

$AA101.\ p_{107}=p_{105}+p_{106}$；$AA102.\ u_{31}=f_5-p_{107}$.

变量：$z_0, w, u_{r0}, u_{t1}, u_{t2}, u_{t3}, v_{t1}, v_{t2}, v_{t3}t_{34}, t_{35}, u_{31}, u_{32}$.

第十四轮

$AM62.\ p_{111}=t_{35}v_{t1}$；$AM63.\ p_{110}=u_{31}u_{t3}$；

$AM64.\ p_{88}=t_{34}u_{r0}$；$AM65.\ p_{108}=v_{t2}^2$；$AM66.\ p_{109}=u_{32}u_{t2}$.

变量：$z_0, w, u_{t1}, v_{t1}, v_{t2}, v_{t3}, p_{88}, p_{108}, p_{109}, p_{110}, p_{111}, u_{31}, u_{32}$.

$AA103.\ p_{112}=p_{108}+u_{t1}$；$AA104.\ p_{113}=p_{109}+p_{112}$；

$AA105.\ p_{114}=p_{113}+p_{110}$；$AA106.\ p_{115}=p_{111}+p_{114}$；

$AA107.\ u_{30}=f_4-p_{115}$；$AA108.\ p_{89}=p_{88}+z_0$.

变量：$w, v_{t1}, v_{t2}, v_{t3}, p_{89}, u_{30}, u_{31}, u_{32}$.

第十五轮

$AM67.\ p_{118}=u_{30}v_{t3}$；$AM68.\ p_{117}=u_{31}v_{t3}$；

$AM69.\ p_{90}=wp_{89}$；$AM70.\ p_{116}=u_{32}v_{t3}$.

变量：$v_{t1}, v_{t2}, p_{90}, p_{116}, p_{117}, p_{118}, u_{30}, u_{31}, u_{32}$.

$AA109.\ v_{32}=v_{t2}-p_{116}$；$AA110.\ v_{31}=v_{t1}-p_{117}$；

$AA111.\ v_{t0}=p_{90}+v_{10}$；$AA12.\ v_{30}=v_{t0}-p_{118}$.

变量：$u_{30}, u_{31}, u_{32}, v_{30}, v_{31}, v_{32}$.

2. 倍点算法

输入：亏格为 3 的超椭圆曲线 $C: y^2=x^7+f_5x^5+f_4x^4+f_3x^3+f_2x^2+f_1x+f_0$；归约除子 $D_1=(U_1, V_1)$，$U_1=x^3+u_{12}x^2+u_{11}x+u_{10}$，$V_1=v_{12}x^2+v_{11}x+v_{10}$，

输出：$D_2=(U_2, V_2)=2D_1$，$U_2=x^3+u_{22}x^2+u_{21}x+u_{20}$，$V_2=v_{22}x^2+v_{21}x+v_{20}$；

初始变量：$u_{12}, u_{11}, u_{10}, v_{12}, v_{11}, v_{10}$。

第一轮

$DM01.\ p_1=u_{11}v_{10}$；$DM02.\ p_2=u_{10}v_{11}$；

$DM03.\ p_3=u_{12}v_{10}$；$DM04.\ p_4=u_{10}v_{12}$；

$DM05.\ p_5=u_{12}v_{11}$；$DM06.\ p_6=u_{11}v_{12}$.

变量：$p_1, p_2, p_3, p_4, p_5, p_6$.

$DA01.\ t_1=p_1-p_2$；$DA02.\ t_2=p_3-p_4$；

$DA03.\ p_7=v_{10}+p_5$；$DA04.\ t_5=p_7-p_6$.

变量：$t_1, t_2, t_5$.

第二轮

$DM07.\ t_{13}=u_{12}^2$；$DM08.\ p_{16}=v_{12}t_5$；

$DM09.\ p_{10}=v_{12}t_2$；$DM10.\ p_8=v_{10}^2$；

$DM11.\ t_3=v_{11}^2$；$DM12.\ t_4=v_{10}v_{11}$；$DM13.\ p_9=v_{12}t_1$.

变量：$p_8, p_9, p_{10}, p_{16}, t_1, t_2, t_3, t_4, t_{13}$.

$DA05.\ t_6=p_8-p_9$；$DA06.\ i_2=t_3-p_{16}$；

$DA07.\ t_7=p_{10}-t_4$；$DA08.\ t_{12}=2u_{11}$；

$DA09.\ p_{23}=f_5+t_{13}$；$DA10.\ t_{15}=p_{23}-t_{12}$；

$DA11.\ p_{25}=t_{12}-t_{15}$；$DA12.\ p_{24}=2t_{13}$；

$DA13.\ z_2=t_{15}+p_{24}$；$DA14.\ p_{12}=t_7-t_4$.

变量：$i_2, z_2, t_{15}, t_{13}, t_1, t_2, t_3, t_5, t_6, t_7, p_{12}, p_{25}$.

第三轮

$DM14.\ t_{23}=i_2z_2$；$DM15.\ p_{26}=u_{12}p_{25}$；

$DM16.\ p_{21}=v_{12}^2$；$DM17.\ p_{19}=u_{12}t_7$；

$DM18.\ p_{18}=u_{11}i_2$；$DM19.\ p_{17}=u_{12}i_2$；$DM20.\ p_{11}=t_5t_6$.

变量：$z_2, p_{11}, p_{12}, p_{17}, p_{18}, p_{19}, p_{21}, p_{26}, i_2, t_1, t_2, t_3, t_6, t_7, t_{13}, t_{15}, t_{23}$.

$DM15.\ p_{27}=t_{15}-u_{11}$；$DA16.\ t_{11}=2u_{10}$；

$DA17.\ p_{22}=t_{11}+p_{21}$；$DA18.\ t_{14}=f_4-p_{22}$；

$DA19.\ p_{29}=t_{11}-t_{14}$；$DA20.\ p_{31}=u_{11}-f_5$；

$DA21.\ t_{20}=2v_{12}$；$DA22.\ i_1=p_{17}+t_7$；

$DA23.\ z_1=p_{26}+t_{14}$；$DA24.\ p_{37}=i_1+i_2$；

$DA25.\ p_{38}=z_1+z_2$；$DA26.\ p_{20}=p_{18}+p_{19}$；

$DA27.\ i_0=t_6+p_{20}$；$DA28.\ p_{43}=i_0+i_2$；

$DA29.\ p_{52}=i_0+i_1$.

变量：$i_0, i_1, z_1, z_2, p_{11}, p_{12}, p_{27}, p_{29}, p_{31}, p_{37}, p_{38}, p_{43}, p_{52}, t_1, t_2, t_3, t_{13}, t_{20}, t_{23}$.

第四轮

$DM21.\ p_{28}=t_{13}p_{27}$；$DM22.\ p_{30}=u_{12}p_{29}$；

$DM23.\ p_{32}=u_{11}p_{31}$；$DM24.\ p_{33}=t_{20}v_{11}$；

$DM25.\ t_{21}=i_1z_1$；$DM26.\ t_{24}=u_{12}t_{23}$；$DM27.\ p_{39}=p_{37}p_{38}$.

变量：$i_0, z_1, z_2, p_{11}, p_{12}, p_{28}, p_{30}, p_{32}, p_{33}, p_{39}, p_{43}, p_{52}, t_1, t_2, t_3, t_{20}, t_{21}, t_{23}, t_{24}$.

$DA30.\ p_{34}=f_3+p_{28}$；$DA31.\ p_{35}=p_{34}+p_{30}$；

$DA32.\ p_{36}=p_{35}+p_{32}$；$DA33.\ z_0=p_{36}-p_{33}$；

$DA34.\ p_{40}=t_{21}+t_{24}$；$DA35.\ p_{41}=p_{39}-p_{40}$；

$DA36.\ t_{25}=p_{41}-t_{23}$；$DA37.\ t_{27}=u_{10}+u_{12}$；

$DA38.\ t_{28}=t_{27}+u_{11}$；$DA39.\ t_{29}=t_{27}-u_{11}$；

$DA40.\ p_{42}=t_{25}-t_{23}$；$DA41.\ p_{44}=z_0+z_2$；

$DA42.\ p_{53}=z_0+z_1$.

变量：$i_0, z_0, p_{11}, p_{12}, p_{41}, p_{42}, p_{43}, p_{44}, p_{52}, p_{53}, t_1, t_2, t_3, t_{20}, t_{21}, t_{23}, t_{24}, t_{25}, t_{28}, t_{29}$.

第五轮

$DM28.\ p_{13}=t_2p_{12}$；$DM29.\ p_{14}=t_1t_3$；

$DM30.\ t_{22}=i_0z_0$；$DM31.\ t_{26}=u_{10}t_{25}$；

$DM32.\ t_{30}=p_{41}t_{28}$. $DM33.\ p=t_{29}p_{42}$.

$DM34.\ p_{45}=p_{43}p_{44}$.

变量：$p, p_{11}, p_{13}, p_{14}, p_{45}, p_{52}, p_{53}, t_{20}, t_{21}, t_{22}, t_{23}, t_{24}, t_{26}, t_{28}, t_{29}, t_{30}$.

$DA43.\ p_{15}=p_{11}+p_{13}$；$DA44.\ r=p_{14}+p_{15}$；

$DA45.\ t_{31}=2r$；$DA46.\ p_{46}=t_{30}+p$；

$DA47.\ p_{47}=p_{46}/2$；$DA48.\ p_{48}=t_{22}+t_{23}$；

$DA49.\ p_{49}=p_{47}+p_{48}$；$DA50.\ p_{50}=t_{21}+t_{26}$；

$DA51.\ p_{51}=p_{45}+p_{50}$；$DA52.\ s'_2=p_{51}-p_{49}$；

$DA53.\ p_{57}=t_{21}+t_{22}$；$DA54.\ p_{55}=p-t_{30}$；

$DA55.\ s'_0=t_{22}-t_{26}$.

变量：$s'_0, s'_2, p_{52}, p_{53}, p_{55}, p_{57}, p_{60}, t_{20}, t_{24}, t_{28}, t_{29}, t_{31}$.

第六轮

$DM35.\ p_{60}=t_{31}s'_2$.

第七轮

$DI.\ t_{32}=p_{60}^{-1}$.

变量：$t_{32}, s'_0, s'_2, p_{52}, p_{53}, p_{55}, p_{57}, t_{20}, t_{24}, t_{28}, t_{29}, t_{31}$.

第八轮

$DM36.\ t_{33}=t_{31}t_{32}$；$DM37.\ p_{54}=p_{52}p_{53}$.

变量：$t_{33}, t_{32}, s'_0, s'_2, p_{54}, p_{55}, p_{57}, t_{31}, t_{20}, t_{24}, t_{28}, t_{29}$.

$DA56.\ p_{58}=p_{54}+t_{24}$；$DA57.\ p_{56}=p_{55}/2$；

$DA58.\ p_{59}=p_{56}+p_{58}$；$DA59.\ s'_1=p_{59}-_{57}$.

变量：$s'_0, s'_1, s'_2, t_{20}, t_{28}, t_{29}, t_{31}, t_{32}, t_{33}$.

第九轮

$DM38.\ p_{61}=s'_2$；$DM39.\ s'_0=t_{33}s'_0$；$DM40.\ s_1=t_{33}s'_1$；

变量：$s_0, s_1, p_{61}, t_{20}, t_{28}, t_{29}, t_{31}, t_{32}, t_{33}$.

$DA60.\ p_{62}=s_0+s_1$；$DA61.\ p_{63}=s_0-s_1$；

$DA62.\ u_{t3}=2s_1$；$DA63.\ g_4=u_{12}+s_1$；

$DA64.\ t_{51}=u_{t3}-g_4$；

变量：$s_0, s_1, u_{t3}, p_{61}, p_{62}, p_{63}, t_{20}, t_{28}, t_{29}, t_{31}, t_{32}, t_{33}, t_{51}$.

第十轮

$DM41.\ w=t_{32}p_{61}$；$DM42.\ \omega_i=t_{31}t_{33}$；

$DM43.\ t_{41}=t_{28}p_{62}$ $DM44.\ t_{42}=t_{29}p_{63}$；

$DM45.\ t_{43}=u_{12}s_1$；$DM46.\ p_{70}=s_1^2$；$DM47.\ p_{94}=t_{51}u_{t3}$.

变量：$\omega_i, s_0, s_1, w, u_{t3}, p_{70}, p_{94}, t_{20}, t_{41}, t_{42}, t_{43}, t_{51}$.

$DA65.\ p_{73}=t_{20}-\omega_i$；$DA66.\ p_{76}=s_1-u_{12}$；

$DA67.\ p_{71}=2s_0$； $DA68.\ u_{t2}=p_{70}+p_{71}$；

$DA69.\ p_{69}=u_{11}+s_0$；$DA70.\ g_3=t_{43}+p_{69}$；

$DA71.\ p_{95}=p_{94}+g_3$；$DA72.\ p_{96}=p_{95}-u_{t2}$；

$DA73.\ p_{66}=t_{41}+t_{42}$；$DA74.\ p_{64}=t_{41}-t_{42}$；

$DA75.\ p_{65}=p_{64}/2$；$DA76.\ g_1=p_{65}-t_{43}$.

变量：$\omega_i, w, s_0, g_1, u_{t2}, u_{t3}, p_{66}, p_{73}, p_{76}, p_{96}, t_{51}$.

第十一轮

$DM48.\ g_0=u_{10}s_0$；$DM49.\ p_{72}=u_{t3}s_0$；

$DM50.\ p_{74}=\omega_i p_{73}$；$DM51.\ p_{77}=p_{76}v_{12}$；

$DM52.\ p_{78}=\omega_i u_{12}$；$DM53.\ p_{90}=t_{51}u_{t2}$；$DM54.\ v_{t3}=wp_{96}$.

变量：$\omega_i, s_0, w, g_0, g_1, u_{t2}, u_{t3}, v_{t3}, p_{66}, p_{72}, p_{74}, p_{77}, p_{78}, p_{90}, t_{51}$.

$DA77.\ p_{79}=p_{77}+v_{11}$；$DA78.\ p_{80}=p_{78}+p_{79}$；

$DA79.\ u_{t1}=p_{72}+p_{74}$；$DA80.\ p_{67}=p_{66}/2$；

$DA81.\ p_{68}=p_{67}+u_{10}$；$DA82.\ g_2=p_{68}-g_0$；

$DA83.\ p_{91}=p_{90}+g_2$ $DA84.\ p_{92}=p_{91}-u_{t1}$.

变量：$g_0, g_1, \omega_i, w, s_0, u_{t1}, u_{t2}, u_{t3}, v_{t3}, p_{80}, p_{92}, t_{51}$.

第十二轮

$DM55.\ p_{75}=s_0^2$；$DM56.\ p_{81}=\omega_i p_{80}$；$DM57.\ p_{86}=t_{51}u_{t1}$；

$DM58.\ p_{93}=wp_{92}$；$DM59.\ p_{97}=v_{t3}^2$.

变量：$g_0, g_1, w, u_{t1}, u_{t2}, u_{t3}, v_{t3}, p_{75}, p_{81}, p_{86}, p_{93}, p_{97}, t_{51}$.

$DA85.\ p_{82}=2p_{81}$；$DA86.\ u_{t0}=p_{75}+p_{82}$；

$DA87.\ p_{87}=g_1-u_{10}$ $DA88.\ p_{88}=p_{86}+p_{87}$；

$DA89.\ p_{98}=u_{t3}+p_{97}$；$DA90.\ u_{22}=-p_{98}$；

$DA91.\ t_{61}=2v_{t3}$；$DA92.\ v_{t2}=p_{93}+v_{12}$.

变量：$g_0, w, u_{t0}, u_{t1}, u_{t2}, u_{t3}, v_{t2}, v_{t3}, p_{88}, t_{51}, t_{61}, u_{22}$.

第十三轮

$DM60.\ p_{89}=wp_{88}$；$DM61.\ p_{99}=u_{22}u_{t3}$；

$DM62.\ p_{100}=t_{61}v_{t2}$.

变量：$g_0, w, u_{t0}, u_{t1}, u_{t2}, u_{t3}, v_{t2}, v_{t3}, p_{89}, p_{99}, p_{100}, t_{51}, t_{61}, u_{22}$.

$DA93.\ p_{101}=u_{12}+p_{99}$；$DA94.\ p_{102}=p_{101}+p_{100}$；

$DA95.\ u_{21}=f_5-p_{102}$；$DA96.\ v_{t1}=p_{89}+v_{11}$.

变量：$g_0, w, u_{t0}, u_{t1}, u_{t2}, u_{t3}, v_{t1}, v_{t2}, v_{t3}t_{51}, t_{61}, u_{21}, u_{22}$.

第十四轮

$DM63.\ p_{106}=t_{61}v_{t1}$；$DM64.\ p_{105}=u_{21}, u_{t3}$；

$DM65.\ p_{83}=t_{51}u_{t0}$；$DM66.\ p_{103}=v_{t2}^2$；$DM67.\ p_{104}=u_{22}u_{t2}$.

变量：$g_0, w, u_{t1}, v_{t1}, v_{t2}, v_{t3}, p_{83}, p_{83}, p_{103}, p_{104}, p_{105}, p_{106}, u_{21}, u_{22}$.

$DA97.\ p_{107}=p_{103}+u_{t1}$；$DA98.\ p_{108}=p_{108}=p_{104}+p_{107}$；

$DA99.\ p_{109}=p_{108}+p_{105}$；

$DA100.\ p_{110}=p_{109}+p_{106}$；$DA101.\ u_{20}=f_4-p_{110}$；

$DA102.\ p_{84}=p_{83}+g_0$.

变量：$w, v_{t1}, v_{t2}, v_{t3}, p_{84}, u_{20}, u_{21}, u_{22}$.

第十五轮

$DM68.\ p_{113}=u_{20}v_{t3}$；$DM69.\ p_{112}=u_{21}v_{t3}$；

$DM70.\ p_{85}=wp_{84}$；$DM71.\ p_{111}=u_{22}v_{t3}$.

变量：$v_{t1}, v_{t2}, p_{85}, p_{111}, p_{112}, p_{113}, u_{20}, u_{21}, u_{22}$.

$DA103.\ v_{22}=v_{t2}-p_{111}$；$DA104.\ v_{21}=v_{t1}-p_{112}$；

$DA105.\ v_{t0}=p_{85}+v_{10}$；$DA106.\ v_{20}=v_{t0}-p_{113}$.

变量：$u_{20}, u_{21}, u_{22}, v_{20}, v_{21}, v_{22}$.

---

（上接第 71 页）

询时间都比 PHT 的查询时间要短。这是由于在 DRT 方法中，可以在非叶节点中存放 key 值，只需找到分配节点之后就可以执行并行查询，而在 PHT 方法中，必须在二叉平衡树中顺序执行，找到所有的叶子节点，然后执行查询，因此，DRT 的耗费的查询时间比 PHT 要少，而且，由于在非叶节点上设置了存放 key 数目的阈值，不会很大地增加存储空间。

**结论** 在已有的 DHT 结构化 P2P 网络之上支持范围查询依然比较困难。本文提出一种基于分布式范围树的结构化 P2P 范围查询方法。该方法将多维索引的分布式范围树分发到已有的结构化 DHT 覆盖网络中，充分利用 DHT 系统提供的简单数据查找接口，可以有效地实现数据对象的范围查询。一维数据集上不同的查询范围的实验结构表明，DRT 方法所需的查询时间比 PHT 更少。更高维数据集对 DRT 方法的性能影响是我们后续的研究中需要考虑的问题。

## 参 考 文 献


1 Stoica I, Morris R, Karger D, et al. Chord: A scalable peer-to-peer lookup service for internet applications. In: Proceeding of the ACM SIGCOMM Conference, San Diego, CA, 2001. 149～160

2 Ratnasamy S, Francis P, Handley M, et al. A scalable content-addressable network. In: Proceeding of the ACM SIGCOMM, San Diego, CA, 2001. 161～172

3 Rowstron A, Druschel P. Pastry: Scalable, distributed object location and routing for large-scale peer-to-peer systems. LNCS, 2001, 2218: 329～350

4 Zhao B Y, Kubiatowicz J D, Joseph A D. Tapestry: An infrastructure for fault-tolerant wide-area location and routing. Berkeley Computer Science Division, University of California, CA: [Technical Report CSD-01-1141]. 2001

5 Harren M, Hellerstein J M, Huebsch R. Complex Queries in DHT-based Peer-to-Peer Networks. In: Proceeding of IPTPS02, Cambridge, USA, 242～259

6 Triantafillou P, Pitoura T. Towards a Unifying Framework for Complex Query Processing over Structured Peer-to-Peer Data Networks[C]. In: Proceedings of the First International Workshop on Databases, Information Systems and Peer-to-Peer Computing (DBISP2P), Berlin, Germany, 2003. 169～183

7 Chawathe Y, Ramabhadran S, Ratnasamy S, et al. A case study in building layered DHT applications. In: Proceedings of the ACM SIGCOMM, Philadelphia, Pennsylvania, USA, 2005. 97～108

8 Bharambe A R, Agrawal M, Seshan S. Mercury: Supporting scalable multi-attribute range queries. In: Proceedings of the ACM SIGCOMM, Portland, USA, 2004. 353～366

9 Harvey N, Jones M, Saroiu S, et al. SkipNet: A Scalable Overlay Network with Practical Locality Properties. In: Proceedings of the Fourth USENIX Symposium on Internet Technologies and Systems, Seattle, WA, March 2003

10 周培德. 计算几何----算法分析与设计. 清华大学出版社, 2000

11 de Berg M, van Kreveld M, Overmars M, Schwarzkopf O. Computational Geometry: Algorithm and Application, second, revised edition. Springer-Verlag, Berlin, 2000

12 Rhea S, Godfrey B, Karp B, et al. OpenDHT: a public DHT service and its uses. In: Proceedings of the ACM SIGCOMM, 2005