УДК 004.056.55

ИСПОЛЬЗОВАНИЕ ДЕТЕРМИНИРОВАННОЙ ФУНКЦИИ РАЗБИЕНИЯ НА МНОЖЕСТВА ДЛЯ РАСПАРАЛЛЕЛИВАНИЯ ρ-МЕТОДА ПОЛЛАРДА[1]

Е.Г. Качко, К.А. Погребняк

В работе предлагается усовершенствованный метод распараллеливания алгоритма Полларда решения задачи дискретного логарифмирования в группе точек эллиптической кривой и в мультипликативной группе конечного поля для систем с общей памятью. Усовершенствование метода достигается за счет построения детерминированной функции разбиения на множества. Такая функция позволяет организовать два независимых сбалансированных вычислительных потока построения блока элементов группы фиксированной длины. Далее анализируются известные функции итерирования точек в алгоритме Полларда и строится обобщенная детерминированная функция разбиения на множества.

Ключевые слова: дискретный логарифм, метод Полларда, эллиптическая кривая.

Введение

Сегодня широко используются криптографические системы с открытым ключом, стойкость которых основывается на существовании вычислительно сложных задач. К таким задачам относится нахождение дискретного логарифма в конечной абелевой группе. В практических приложениях используются аддитивная группа точек эллиптической кривой, заданной над конечным полем, и мультипликативная группа элементов поля Галуа.

Особый интерес представляют методы решения задачи дискретного логарифмирования. Для вычисления дискретного логарифма в группе точек эллиптической кривой наиболее эффективным считается ρ-метод Полларда, а для решения задачи логарифмирования в мультипликативной группе поля Галуа – метод решета числового поля [1]. Тем не менее, ввиду простоты и универсальности метода Полларда, его часто используют и в мультипликативной группе поля Галуа при небольшой характеристике поля.

Фактически, ρ-метод Полларда состоит из алгоритма построения псевдослучайной последовательности и алгоритма обнаружения коллизии.

В работах [2–4] предложен параллельный ρ-метод Полларда для систем с общей памятью. Недостатком указанного метода является несбалансированность вычислительных потоков при распараллеливании алгоритма построения псевдослучайной последовательности.

В данной работе предлагается усовершенствованный метод распараллеливания алгоритма Полларда решения задачи дискретного логарифмирования в группе точек эллиптической кривой за счет построения детерминированной функции разбиения на множества. Полученный метод также применяется и для мультипликативной группы поля Галуа.

Отметим, что ρ-метод Полларда решения задачи дискретного логарифмирования не зависит от структуры группы, поэтому, в дальнейшем будет выбрана аддитивная форма записи и описано изложение метода для группы точек эллиптической кривой, которое тривиальным образом переносится на случай мультипликативной группы поля Галуа.

[1]Статья рекомендована к публикации программным комитетом международной научной конференции «Параллельные вычислительные технологии 2013»

1. Метод Полларда

Пусть задана группа точек эллиптической кривой, которая будет обозначаться как $E(\mathbb{F}_p)$, такая что $\#E(\mathbb{F}_p) = n \cdot cof$, где n – простое число, cof – небольшое натуральное число. Не ограничивая общности, можно предположить, что $p > 3$ и p – простое число. Обозначим подгруппу $E(\mathbb{F}_p)$ порядка n через G и зафиксируем порождающий элемент P.

Для произвольного элемента группы $Q = xP$ задача дискретного логарифмирования заключается в нахождении элемента $1 < x < n$.

1.1. Последовательный ρ-метод Полларда

Группа G представляется в виде объединения $G = S_1 \cup S_2 \ldots \cup S_N$, где S_i – произвольные множества приблизительно одинаковой мощности, N – натуральное число. Функция итерирования $f : G \to G$ определяется как

$$R_{i+1} = f(R_i) = \begin{cases} Q + R_i, & R_i \in S_1 \\ 2R_i, & R_i \in S_2 \\ P + R_i, & R_i \in S_3 \end{cases}$$

Пусть $R_{i+1} = a_i P + b_i Q$, тогда коэффициенты определяются следующим образом

$$a_{i+1} = \begin{cases} a_i \mod n, & R_i \in S_1 \\ 2a_i \mod n, & R_i \in S_2 \\ a_i + 1 \mod n, & R_i \in S_3 \end{cases}$$

$$b_{i+1} = \begin{cases} b_i + 1 \mod n, & R_i \in S_1 \\ 2b_i \mod n, & R_i \in S_2 \\ b_i \mod n, & R_i \in S_3 \end{cases}$$

Так как группа G – конечна, то последовательность $\{R_i\}_{i=0}^{\infty}$ – периодическая. Таким образом, найдутся два наименьших натуральных числа t и l, таких что $R_t = R_{t+l}$. Фактически, l – означает длину периода последовательности.

Идея алгоритма детектирования цикла Флойда заключается в нахождении индекса i_0, такого что $R_{i_0} = R_{2i_0}$, $i_0 \leq t + l$ при произвольно фиксированном начальном значении R_0.

Отметим, что

$$\begin{aligned} R_i &= f\left(R_{i-1}\right) \\ R_{2i} &= f\left(f\left(R_{i-1}\right)\right) \end{aligned} \tag{1}$$

Это означает, что на каждой итерации производится сравнение R_i и R_{2i} для $0 < i \leq t + l$ пока не будет обнаружена коллизия $R_{i_0} = R_{2i_0}$.

Учитывая, что

$$\begin{aligned} R_{i_0} &= a_{i_0} P + b_{i_0} Q \\ R_{2i_0} &= a_{2i_0} P + b_{2i_0} Q \end{aligned}$$

можно вычислить

$$x = \frac{a_{2i_0} - a_{i_0}}{b_{i_0} - b_{2i_0}}$$

Отметим, что i_0 зависит от начального значения R_0 и определяет вычислительную сложность метода Полларда.

Заметим, что принадлежность $R_i = (x_i, y_i)$ к подмножеству S_j, $1 \le j \le N$ на практике определяется либо младшими, либо старшими разрядами R_i.

Например:

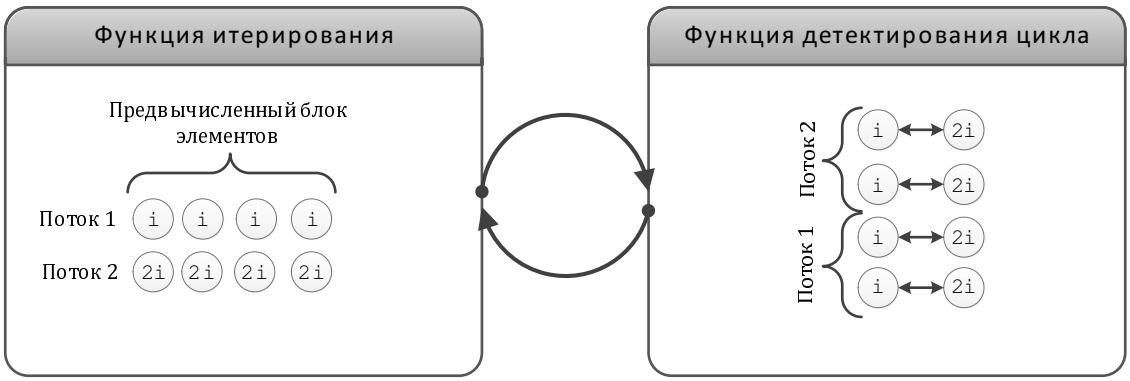
$$j = \nu(R_i) = x_i \mod N + 1,$$

где $\nu : G \to \{1, \dots N\}$ – функция разбиения группы на множества.

1.2. Параллельный ρ-метод Полларда с использованием детерминированной функции разбиения на множества

В работе [3] предложен параллельный ρ-метод Полларда для систем с общей памятью. Идея такого метода заключается в распараллеливании отдельно функции итерирования и алгоритма Флойда детектирования цикла.

Учитывая накладные расходы, связанные с использованием потоков, вычисление и сравнение точек R_i и R_{2i} за одну итерацию является неэффективным. Поэтому, было предложено вычислить блок элементов определенной длины для точек R_i и параллельно вычислить блок элементов для точек R_{2i}, после чего параллельно сравнить элементы, содержащиеся в первой и второй половинах блока, как показано на рисунке.



Параллельный алгоритм Полларда с предвычисленным блоком

Функция итерирования распараллеливается на этапе вычисления последовательностей $\{R_i\}_{i=0}^{m}$ и $\{R_{2i}\}_{i=0}^{m}$. Это достигается организацией вычислений последовательностей вида

$$\{R_{iw+j}\}_{i=0}^{l} \text{ и } \{R_{2(iw+j)}\}_{i=0}^{l}$$

где w – это размер блока вычислений, $0 \le j < w$, $l = \left\lceil \frac{m}{w} \right\rceil$.

Результатом выполнения функции итерирования точек являются два множества точек $\{R_i\}_{i=0}^{w}$ и $\{R_{2i}\}_{i=0}^{w}$, сравнение которых осуществляется по блокам, то есть

$$R_i = R_{2i}, 1 \le i \le \frac{w}{2}$$
$$R_i = R_{2i}, \frac{w}{2} < i \le w$$

Следует отметить, что вычисление точки R_{2i}, согласно формуле (1), требует последовательного вычисления двух образов функции f. Так как функция является итеративной и определяется функцией разбиения группы на множества, то в общем случае нельзя свести

ее к явному представлению в виде композиционной функции. Это означает, что вычисление R_i в одном потоке является в два раза медленнее, чем вычисление R_{2i} в другом.

Для балансировки нагрузки между потоками, желательно представить вычисление двух образов функции f в виде вычисления одного образа композиционной функции. Это может быть достигнуто использованием детерминированной функции разбиения абелевой группы на множества.

Определим детерминированную функцию $\xi : G \to \{1, \dots N\}$ разбиения на множества как

$$j = \xi(R_i) = i \mod N + 1. \tag{2}$$

Такая функция разбиения абелевой группы на множества позволяет сделать предсказание траектории перехода и построить композиционную функцию.

Предложение 1. Пусть задана детерминированная функция разбиения группы на множества $\xi(R_i) = i \mod N + 1$, тогда вычисление R_{2i} может быть представлено как

$$R_{2i} = g(S_{i-1}),$$

где $g : G \to G$, $S_{i-1} = R_{2(i-1)}$.

Доказательство. Определим функцию итерирования g следующим образом:

$$S_{i+1} = g(S_i) = \begin{cases} 2(Q + S_i), & S_i \in S_1 \\ S_i + P + Q, & S_i \in S_2 \\ 2S_i + P, & S_i \in S_3 \end{cases}$$

По определению $R_{2i} = f\left(f\left(R_{i-1}\right)\right)$. Так как функция разбиения группы на множества представлена уравнением (2), то

$$R_{2i} = \begin{cases} 2(R_{2(i-1)} + Q), & R_{2(i-1)} \in S_1 \\ R_{2(i-1)} + P + Q, & R_{2(i-1)} \in S_2 \\ 2R_{2(i-1)} + P, & R_{2(i-1)} \in S_3 \end{cases}$$

Следовательно, $R_{2i} = S_i = g(S_{i-1})$.

Таким образом, вычисление двух итераций функции f может быть сведено к вычислению одного образа функции g с использованием детерминированной функции разбиения группы на множества. □

Отметим также, что изменение псевдослучайной функции итерирования элементов на детерминированную, с одной стороны, влияет на статистические свойства обнаружения коллизии, предположительно, в худшую сторону, а с другой стороны, ведет к балансировке потоков при построении блока элементов и, следовательно, к уменьшению общей вычислительной нагрузки алгоритма Полларда.

1.3. Обобщение метода Полларда с детерминированной функцией разбиения на множества на произвольную функцию итерирования

Рассмотрим известные модификации [1] функции итерирования для последовательного алгоритма Полларда, а именно, обобщенную функцию итерирования Полларда, функцию итерирования Теске и смешанную функцию итерирования Теске.

Обобщенная функция итерирования Полларда представляется в виде:

$$R_{i+1} = f_{PG}(R_i) = \begin{cases} W_1 + R_i, & R_i \in S_1 \\ 2R_i, & R_i \in S_2 \\ W_2 + R_i, & R_i \in S_3 \end{cases}$$

где $W_1 = t_1 P$, $W_2 = t_2 Q$, t_1,t_2 - случайным образом выбранные числа, такие что $0 < t_1, t_2 \leq n$.

Предположим, что предварительно вычислено r значений $W_i = t_i^1 P + t_i^2 Q$, $i = 1..r$. Определим функцию $\nu : G \to \{1..r\}$, тогда функция итерирования Теске может быть описана следующим образом:

$$R_{i+1} = f_{TA}(R_i) = R_i \cdot W_{\nu(R_i)}, \nu(R_i) \in 1..r$$

Смешанная функция итерирования Теске записывается как:

$$R_{i+1} = f_{TM}(R_i) = \begin{cases} R_i \cdot W_{\nu(R_i)}, & \nu(R_i) \in 1..r \\ 2R_i, & \nu(R_i) \notin 1..r \end{cases}$$

Отметим, что исходя из представления функций, тривиальным образом можно распространить идею алгоритма Полларда для систем с общей памятью с использованием детерминированной функции разбиения на множества, а именно, выполнять последовательный переход от одного подмножества к другому.

Такой подход позволит предсказывать траекторию движения функции итерирования, что даст возможность организовывать балансировку потоков более оптимальным способом.

2. Результаты моделирования ρ-метода Полларда с использованием детерминированной функции разбиения на множества

Для реализации описанных выше алгоритмов использовались: процессор Intel (R) Core (TM)2 Duo CPU E6850 3.00GHz, ОЗУ – 2Gb , ОС – Windows 7. Ограничение случаем для двуядерных процессоров вызвано тем, что итерируются параллельно не более двух последовательностей.

В таблице приведено время выполнения в секундах (δ_t) для последовательного и параллельного методов Полларда для систем с общей памятью. Временная оценка проводится в зависимости от длины блока согласно алгоритму на рисунке.

Отметим, что детерминированная функция разбиения группы на множества позволила при программной реализации использовать две независимых функции итерирования для вычисления R_i и R_{2i}, использовать предвычисления в функции итерирования g для значения $P + Q$, а также отказаться от условных операторов при определении принадлежности

Таблица

Временные показатели методов Полларда

№ п/п	Методы Полларда	δ_t (с)	
		21 бит	**27 бит**
1	Классический метод	12.4141	1069.49
2	Параллельный метод (w=1)	9.6856	890.812
3	Параллельный метод (w=4)	8.70438	765.313
4	Параллельный метод (w=8)	8.45161	786.541
5	Параллельный метод (w=128)	8.21501	810.267
6	Параллельный метод (w=512)	8.17755	726.259
7	Параллельный метод (w=1024)	8.1422	706.71
8	Параллельный метод (w=2048)	8.1446	702
9	Параллельный метод (w=4096)	8.21867	706.509

точки R_i множеству S_i, что позволило минимизировать потери, связанные с неправильным предсказанием переходов и в полной мере использовать параллельные вычисления.

Заключение

В работе предложен метод распараллеливания алгоритма Полларда решения задачи дискретного логарифмирования в группе точек эллиптической кривой для систем с общей памятью с использованием детерминированной функции разбиения абелевой группы на множества. Такой подход позволяет оптимально использовать преимущества как многопроцессорных, так и многоядерных систем. В работе приведены эмпирические временные показатели для предложенного параллельного метода Полларда. Моделирование проводилось для двухъядерных процессоров, что обусловлено наличием двух последовательностей в алгоритме обнаружения цикла. Предложенный подход к распараллеливанию алгоритма Полларда позволил снизить время вычислений на 30 %.

Следует отметить, что сравнение производилось для псевдослучайной функции итерирования и детерминированной для нескольких начальных значений. Такое сравнение не позволяет полноценно сделать вывод о степени ухудшения или улучшения статистических характеристик метода Полларда.

В дальнейшем планируется обобщить полученные результаты на случай произвольного числа ядер и на кривые с большей битовой длиной порядка подгруппы, а также рассмотреть другие варианты детерминированных функций.

Отметим также, что анализировался только один алгоритм обнаружения цикла, а именно алгоритм Флойда [1]. Необходимо также проанализировать альтернативные алгоритмы, например, алгоритм Брента [1]. Структура алгоритма Брента смогла бы позволить построить конвейер вычислений, на котором при вычислении следующего блока точек ЭК на одном ядре, происходит поиск коллизии на другом.

В дальнейшем также необходимо исследовать влияние начального значения для функции итерирования на выбор длины блока. Отметим, что исходя из экспериментальных данных, оптимальной длиной блока является $w = 512$ или $w = 1024$.

Литература

1. Bai, S. On the efficiency of Pollard's rho method for discrete logarithms / S. Bai, R. P. Brent // Fourteenth Computing: The Australasian Theory Symposium (CATS 2008), January 22–25, 2008, Wollongong, NSW, Australia, Proceedings. CRPIT, 77. Harland J. and Manyem P., Eds. ACS. P. 125–131.

2. Качко, Е.Г. Параллельный метод Полларда решения задачи дискретного логарифмирования в группе точек эллиптической кривой / Е.Г. Качко, К.А. Погребняк // Параллельные вычислительные технологии (ПАВТ–2012): труды международной научной конференции (Новосибирск, 26–30 марта, 2012 г.). – Челябинск: Издательский центр ЮУрГУ, 2012. – С. 723.

3. Горбенко, И.Д. Методы распараллеливания алгоритма Полларда решения задачи дискретного логарифмирования для систем с общей памятью / И.Д. Горбенко, Е.Г. Качко, К.А. Погребняк // Высокопродуктивные вычисления (HPC–UA'2012): труды международной научной конференции (Киев, 8–10 октября, 2012 г.). – Киев: НАНУ, 2012. – С. 152–157.

4. Горбенко, И.Д. Параллельный метод Полларда решения задачи дискретного логарифмирования в мультипликативной группе поля Галуа / И.Д. Горбенко, Е.Г. Качко, К.А. Погребняк // Современные проблемы информационной безопасности на транспорте (СПИБТ–2012): материалы всеукраинской научно-технической конференции с международным участием (Николаев, 29–30 ноября, 2012 г.). – Николаев: НУК, 2012. – С. 9–11.

Елена Григорьевна Качко, кандидат технических наук, профессор, кафедра «Программная инженерия», Харьковский национальный университет радиоэлектроники (г. Харьков, Украина), ekachko@gmail.com.

Константин Анатольевич Погребняк, кандидат технических наук, кафедра «Безопасность информационных технологий», Харьковский национальный университет радиоэлектроники (г. Харьков, Украина), iitkostya@gmail.com.

USING A DETERMINISTIC PARTITIONING FUNCTION FOR POLLARD'S RHO METHOD PARALELLIZATION

E.G. Kachko, Kharkov National University of Radioelectronics (Kharkov, Ukraine)**,**
K.A. Pogrebnyak, Kharkov National University of Radioelectronics (Kharkov, Ukraine)

An improved method for parallelization of Pollard's algorithm for solving the discrete logarithm problem in a group of elliptic curve points and in a multiplicative group of a Galois field for shared memory systems is suggested in the paper. Improvement of the method is achieved by constructing a deterministic partitioning function. Such a function allows to organize two independent load balancing computational threads for building a block of group elements of fixed length. Also we analyze advanced iteration functions for Pollard's algorithm and build generic deterministic partitioning function.

Keywords: discrete logarithm, Pollard's rho method, elliptic curve.

References

1. Bai S., Brent R.P. On the Efficiency of Pollard's Rho Method for Discrete Logarithms // Fourteenth Computing: The Australasian Theory Symposium (CATS 2008), January 22–25, 2008, Wollongong, NSW, Australia, *Proceedings.* CRPIT, 77. Harland J. and Manyem P., Eds. ACS. P. 125–131.
2. Kachko E.G., Pogrebnyak K.A. Parallelniy metod Pollarda resheniya zadachi diskretnogo logarifmirovaniya v gruppe tochek elipticheskoy krivoy [Parallelized Pollard's Method for Solving the Elliptic Curve Discrete Logatrithm Problem] // Parallelniye vichislitelniye tekhnologii (PAVT–2012): trudy mezhdunarodnoy nauchnoy konferentsii [Proceedings of the International Scientific Conference «Parallel Computational Technologies (PCT–2012)»], March 26–30, 2012, Novosibirsk, *Proceedings.* – Chelyabinsk: YUrGU Publ., 2012. – P. 723.
3. Gorbenko I.D., Kachko E.G., Pogrebnyak K.A. Metody rasparallelivaniya algoritma Pollarda resheniya zadachi diskretnogo logarifmirivaniya dlya sistem s obshey pamyatyu [Methods of Parallelization of Pollard's Algorithm for Solving the Discrete Logarithm Problem for Shared Memory Systems] // Vysokoproductivniye vichisleniya (HPC–UA'2012): trudy mezhdunarodnoy nauchnoy konferentsii [Proceedings of the International Scientific Conference «High performance computing (HPC–UA'2012)»], October 8–10, 2012, Kiev, *Proceedings.* – Kiev: NANU, 2012. P. 152–157.
4. Gorbenko I.D., Kachko E.G., Pogrebnyak K.A. Parallelniy metod Pollarda resheniya zadachi diskretnogo logarifmirovaniya v multiplikativnoy gruppe polya Galua [Parallelized Pollard's Method for Solving the Discrete Logatrithm Problem in the Multiplicative Group of a Galois Field] // Sovremenniye problemy informatsionnoy bezopasnosti na transporte (SPIBT–2012): materialy vseukrainskoy nauchno-tekhnicheskoy konferentsii s mezhdunarodnym uchastiem [Proceedings of the Scientific Conference «Modern problems of information security on transport»], November 29–30, 2012, Nikolaev, *Proceedings.* – Nikolaev: NUK, 2012. – P. 9–11.

Поступила в редакцию 19 апреля 2013 г.