Параллельный метод Полларда решения задачи дискретного логарифмирования в группе точек эллиптической кривой

Е.Г. Качко, К.А. Погребняк

Харьковский национальный университет радиоэлектроники

Известно, что стойкость значительной части криптографических примитивов, используемых в информационных системах, основывается на вычислительной сложности решения задачи дискретного логарифма в группе точек эллиптической кривой (ЭК), заданной над конечным полем. Методы дискретного логарифмирования в группе точек ЭК принято разделять на два типа. К первому типу относятся методы, которые применимы к ЭК с определенной структурой группы, а ко второму – методы логарифмирования для произвольной структуры группы. Следует отметить, что при правильном выборе ЭК атаки первого типа становятся нереализуемыми. Среди методов логарифмирования второго типа, наиболее эффективным считается вероятностный метод Полларда [1]. Фактически, метод Полларда включает в себя алгоритм построения псевдослучайной последовательности точек ЭК и алгоритм обнаружения коллизии. Повышение эффективности криптоанализа методом Полларда достигается за счет сокращения длины последовательности значений функции итерирования, улучшения алгоритма обнаружения коллизии и распараллеливания вычислений. Идея распараллеливания метода Полларда состоит в том, что итерирование точек возлагается на клиентские рабочие станции, а обнаружение коллизии – на сервер [2]. Предложенный параллельный метод Полларда предполагает наличие высокопроизводительных сетей и не учитывает использование многоядерной архитектуры клиентских рабочих станций и сервера. Таким образом, актуальной задачей является исследование известных модификаций метода Полларда и адаптации их к многоядерной архитектуре рабочих станций.

В работе предложен метод распараллеливания алгоритма Полларда решения задачи дискретного логарифмирования в группе точек эллиптической кривой для систем с общей памятью. На основе параллельного алгоритма Ооршота и Вейнера [2] для систем с распределенной памятью предложен комбинированный метод нахождения дискретного логарифма, который позволяет использовать преимущества как многопроцессорных, так и многоядерных систем. Проанализированы известные функции итерирования точек в алгоритме Полларда и построен обобщенный метод Полларда для произвольной функции итерирования и систем с общей памятью. Приведены аналитические выражения для предложенных параллельного метода Полларда и комбинированного метода Полларда для двуядерных процессоров. В работе получены эмпирические временные показатели для параллельного метода Полларда для систем с общей памятью для битовой длины порядка группы точек ЭК 21, 23 и 32 бита, которые согласуются с аналитическими выражениями. Следует отметить, что моделирование проводилось для двуядерных процессоров, что обусловлено наличием двух последовательностей в алгоритме обнаружения цикла. Предложенный подход к распараллеливанию алгоритма Полларда позволил снизить время вычислений на 30 – 50%. Исследованы временные показатели избыточных операций для параллельного алгоритма Полларда для систем с общей памятью.

В дальнейшем планируется провести моделирование для комбинированного метода и для различных итеративных функций, обобщить полученные результаты на случай произвольного числа ядер и на кривые с большей битовой длиной порядка подгруппы.

Литература

1. Pollard J.M. Monte Carlo methods for index calculus computation (mod p) // Mathematics of Computation. July 1978. Vol. 32, No. 143. P. 918-924.
2. P. Van Oorschot, Wiener M. Parallel collision search with cryptanalytic applications. // Journal of Cryptology. 1999. Vol. 12. P. 1–28.