АЛГОРИТМ НАХОЖДЕНИЯ ПОРЯДКА ГРУППЫ ТОЧЕК НА ЭЛЛИПТИЧЕСКОЙ КРИВОЙ

С.Б. САЛОМАТИН, Д.С. ЗЕЛЕНЮК, В.А. СТРИЖЕНОК

Эллиптические кривые над конечными полями являются наиболее перспективной структурой для построения криптографических алгоритмов. Одной из важной задач применения такого рода структур является определения порядка группы точек.

Входными данными для процедуры определения группы точек будут являться нижняя и верхняя границы диапазона, в котором необходимо провести поиск, точка на эллиптической кривой P, переменная из общего уравнения для эллиптической кривой, модуль N, по которому производятся вычисления. Выходными данными в случае отыскания порядка группы точек на заданной эллиптической кривой будет являться сам порядок, содержащийся в переменной либо 0, в случае, когда порядок определить невозможно. Границы диапазона, в котором производится поиск определяются исходя из теоремы Хассе: lowwerbaund=N+1–2 $N^{0,5}$, upperbaund=N+1+ +2 $N^{0,5}$.

Поиск порядка начинается с вычисления точки (lowwerbaund)P и реализуется процедурами kP либо kP2 в зависимости от характеристики поля, в котором производятся вычисления. Характеристика поля учитывается при выборе конкретной эллиптической кривой и определяется непосредственно из коэффициентов a в общей формуле эллиптической кривой.

Для оптимизации алгоритма и уменьшения времени вычисления, каждая новая точка вычисляется уже не с помощью процедур kP либо kP2, а с помощью процедур addec либо addec2, входными данными для которых являются две точки на кривой, которые необходимо сложить, а не одна, как в случае kP (kP2). Таким образом, при каждой итерации вычисление производится не с начальной точкой P, а с точки, соответствующей промежуточному вычисленному значению точки на кривой addp.

При больших степенях такой подход дает выигрыш во времени в 2–3 раза, что существенно ускоряет время выполнения любого алгоритма, базирующегося на отыскании точек эллиптической кривой.