УДК 681.3.06

А.В.Бессалов, Д. Б. Третьяков

Повышение производительности криптоанализа на эллиптической кривой на основе деления точек на два

Предложена реализация метода решения проблемы дискретного логарифмирования на эллиптической кривой над полем $\mathbf{F}_2^m$ *с заменой операций удвоения и сложения точек операцией деления точки на два. Показано, что процедура последовательного деления точки на два в нормальном базисе поля сводится практически к одной операции умножения в поле, т.е. групповая операция по сложности соизмерима с операцией в поле. Это дает рост производительности вычислений до* 2 *порядков.*

Арифметика эллиптических кривих (ЭК) сегодня широко используется в международных и национальных стандартах цифровой пiдписи [1]. Стойкость таких криптосистем основана на сложности решения проблемы дискретного логарифмирования (DLP – Discrete Logarithm Problem) в группе точек ЭК [2 – 4]. Наиболее эффективным здесь пока считается ρ-метод Полларда. Псевдослучайный поиск коллизий этим методом строится на комбинации удвоений-сложений точек кривой. Каждая такая групповая операция над полем $\mathbf{F}_2^m$ весьма трудоемка и достигает около ста операций в поле, эквивалентных умножению. В [2, 4] предложено выполнять решение DLP с использованием более эффективной в сравнении с удвоением операции деления точки на два. В данной работе мы покажем, что переход к одной групповой операции последовательного деления точек на два позволяет реализовать процедуру, подобную алгоритму Шенкса, с многократным ростом скорости криптоанализа.

Рассмотрим несуперсингулярную кривую

$$(1)\quad y^2 + xy = x^3 + ax^2 + b,\quad a, b \in \mathbf{F}_2^m,\ a = 1,\ b \neq 0,$$

с почти простым порядком $N_E = 2n$ (n – простое число) и генератором криптосистемы $G = (x_G, y_G)$ порядка n. Точку $Q = kG$, , образующуюся k- кратным сложением точек G, называют скалярным произведением. При больших n проблема дискретного логарифмирования на ЭК состоит в нахождении целого k при известных G и kG,. Сложность ее решения оценивается как экспоненциальная [2, 3].

Пусть **G** – группа точек криптосистемы порядка n Столько же на ЭК имеется точек максимального порядка $2n$, не входящих в криптосистему. Рассмотрим точки последовательного деления на два Q_0, $Q_1 = Q_0/2$, $Q_2 = Q_1/2,\ldots,Q_i = Q_{i-1}/2 = Q_0/2^{i-1}$, $Q_i \in \mathbf{G}$. Из известных формул удвоения точки [2] при $a = 1$

(2) $x_{i-1} = \nu_i^2 + \nu_i + 1, \qquad \nu_i = x_i + y_i/x_i$,

(3) $y_{i-1} = x_i^2 + x_{i-1}(\nu_i + 1)$,

легко получить обратное решение, дающее координаты 2-х точек деления точки Q_{i-1} на два

(4) $x_i^2 = x_{i-1}(x_{i-1} + \nu_{i-1} + \nu_i + \delta), \quad \delta \in \{0,1\}$

(5) $y_i = x_i^2 + \nu_i x_i$.

Их можно найти, предварительно решив квадратное уравнение (2) над полем $\mathbf{F_2}^m$

(6) $\nu_i^2 + \nu_i + (x_{i-1} + 1) = 0$

относительно неизвестной ν_i . Оно имеет два решения ν_i и $\nu_i + 1$ тогда и только тогда, когда след

(7) $\mathrm{Tr}(x_{i-1} + 1) = 0 \quad \Rightarrow \quad \mathrm{Tr}(x_{i-1}) = 1.$

В нормальном базисе поля, как известно, возведение в квадрат элемента поля сводится к циклическому сдвигу вправо его двоичного векторного представления [2]. Кроме того, при нечетных расширениях m поля след элемента с четным весом (четным числом единиц) равен 0, а след элемента с нечетным весом – 1. Все точки криптосистемы порядка n являются точками делимости на два, тогда как точки максимального порядка $2n$ таковыми не являются (не существуют решения уравнения (6). Это связано с тем, что в мультипликативной группе поля F_n^* все элементы (в том числе 2) имеют обратные по умножению, а в кольце $Z/2n$ четные числа обратных элементов не имеют. Поэтому из двух точек деления на два, имеющих порядки n и $2n$, отбирается согласно (7) точка с нечетным весом x-координаты. Она и является точкой криптосистемы порядка n. Вторая точка деления на два имеет четный вес и, соответственно, порядок $2n$ В уравнение (4) сначала подставляется первое решение уравнения (6) при $\delta = 1$ и находится вес x_i^2. Если он нечетный, значение x_i сразу определяет точку группы $\boldsymbol{G}$ криптосистемы. В противном случае принимается $\delta = 0$ и отбирается вторая точка деления.

Заметим, что определение следа и решение уравнения (6) в нормальном базисе сводятся к побитовому сложению по модулю 2 элементов m-мерного вектора и являются «бесплатными» операциями [2]. Последовательное деление точек на 2 требует, согласно (4), нахождения на каждом шаге пары (x_i,ν_i) вместо (x_i,y_i), что дает сложность групповой операции деления на 2, равную одному умножению M в поле. При необходимости определения y-координаты, согласно (5), потребуется $2M$ умножений. При последовательном поиске коллизий в этом, однако, нет смысла.

Сравним сложность выполнения групповых операций удвоения и деления точки на два. Игнорируя простые операции сложения и обозначая инверсию элемента как I, удвоение точки согласно (2), (3) дает число операций $C = I + 4M$. Инверсия, как известно, является наиболее трудоемкой операцией, эквивалентной (10…80)M [5], при этом C = (14…84)M. Следовательно, переход от операции удвоения к делению точки на 2 повышает скорость анализа в десятки раз (до 2-х порядков).

Рассмотрим варианты поиска коллизий точки $Q = kG$ с использованием деления точек на 2 Пусть при известном s найдены точки $R = sG$ и $P = Q + R = (k + s)G$. Потребуем сначала, чтобы 2 была примитивным элементом группы F_n^*, тогда все точки группы **G** (кроме точки на бесконечности O) представимы как 2^iG, $i = 0, 1,\ldots, n-2$. Их условно можно эквидистантно расположить на окружности в порядке нарастания i. Построим итерационную процедуру из 2-х ветвей

$$(8) \qquad Q_i = Q/2^i, \qquad P_i = P/2^i$$

с двумя возможными коллизиями $Q_i = P_0$ и $P_r = Q_0$ (здесь P_0, Q_0 являются своего рода «маркерами»), откуда получим одно из двух решений

$$(9) \qquad k = s/(1-2^i) \bmod n., \qquad k = s/(2^r - 1) \bmod n\ .$$

Более быстрое решение дают ближе расположенные точки на окружности 2^iG. Далее естественно обобщить процедуру (8) на N маркеров, так что

$$(10) \qquad Q_i = Q/2^i, \qquad P_{ti} = P_t/2^i, \quad t = 1, 2\ ,\ldots, N-1.$$

По сути, данная процедура реализует алгоритм Шенкса, если точки P_t эквидистанты и их число $N \cong \sqrt{n}$. Поскольку метод Шенкса трудно реализуем в связи с проблемой памяти, возможной альтернативой является переход к псевдослучайному поиску коллизий путем соответствующей смены маркеров. Этот путь ведет к усовершенствованному ρ-методу Полларда. Если к операции деления на два добавить сравнительно редкие сложения точек, можно снять ограничение на примитивность элемента 2 мультипликативной группы поля $\mathbf{F}_n$. Операция сложения позволяет псевдослучайно перемещать итерационную процедуру в смежные подгруппы этой группы. Наиболее просто такая процедура может быть задана как

$$(11) \qquad Q_{i+1} = \begin{cases} \delta_i \cdot (Q_i / 2), & \delta_i \in \{0,1\} \\ (1 - \delta_i) \cdot (Q_i + G) \end{cases}$$

Двоичная последовательность δ_i здесь является псевдослучайной с варьируемым распределением символов 1 и 0. Поскольку вычисления более эф-

фективны при преобладаниях 1 в этой последовательности, был проведен статистический анализ среднего числа итераций ν до наступления коллизии от вероятности $\pi = P\{\delta_i = 1\}$ для модели с небольшим значением порядка $n = 1061$ криптосистемы. Данные анализа приведены в таблице 1

Таблица 1

π	1/2	2/3	3/4	4/5	6/7	8/9	10/11	1213
ν	54	63	64	73	80	85	93	104

Данный тренд практически линейно растет с увеличением относительного числа единиц в последовательности δ_i. Он отражает противоречие между производительностью итераций и их числом. Минимальное время успешной атаки, вероятно, следует находить экспериментально для реальных криптосистем и программ криптоанализа.

Теоретическая нижняя граница среднего числа итераций ρ-методом Полларда составляет в нашем примере $\sqrt{\frac{\pi}{2}n} = 41$. Как видим, упрощенный алгоритм (11) проигрывает свыше 30% идеальной модели криптоанализа по числу итераций. Но не следует забывать, что среднее время каждой итерации существенно сокращается за счет применения метода деления точек на два. Классический ρ-метод Полларда предполагает по меньшей мере три ветви итерационной процедуры. Нет сомнения, что рассмотренные алгоритмы с использованием их комбинирования могут быть усовершенствованы.

Литература

1. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка. –К.: Держстандарт України, 2003.–94с.

2. Бессалов А.В. Криптосистемы на эллиптических кривых. Политехника, Киев, 2004. – 224с.

3. N. Koblitz and A.Menezes. Another Look at Non-standard Discrete Log and Diffi-Hellman Problems. CACR 2007−32. http//www.cacr.math.uwaterloo.ca/

4. Бессалов А.В. Метод решения проблемы дискретного логарифмирования на эллиптической кривой путем деления точек на два //Кибернетика и системный анализ.–2001.–№ 6.–С.50–53.

5. K. Fong, D.Hankerson, J.Lopez, A.Menezes. Field Inversion and Point Halving Revisited. Technical Report CORR-2003-18.

1. Опубликована в журнале «Захист інформації,» №4, 2009. С.18-20.