УДК 512.624.95 + 517.772

БЕССАЛОВ А.В., д-р техн.наук, ЧЕВАРДИН В.Е., канд.техн.наук

ОЦЕНКА МОЩНОСТИ МНОЖЕСТВ ТРАНСФОРМАЦИЙ КАНОНИЧЕСКОЙ ФОРМЫ УРАВНЕНИЯ ЭЛЛИПТИЧЕСКОЙ КРИВОЙ

Введение

Начало 80-х годов стало новой ветвью развития несимметричной криптографии. Независимо Миллер и Коблиц предложили использовать эллиптические кривые в криптографических целях. Впоследствии, криптография на эллиптических кривых вызвала большой коммерческий интерес, а позднее, практически, вытеснила с этого рынка RSA-подобные криптосистемы.

Известные протоколы: Диффи-Хеллмана, Эль Гамаля, криптосистема RSA сегодня уже реализованы на преобразованиях в группе точек эллиптической кривой (ЭК). Впоследствии были разработаны и приняты международные и национальные стандарты, определяющие принципы и порядок использования операций в группе точек ЭК. Применение операций в группе точек ЭК позволило сократить вычислительные затраты на криптографические операции генерации и верификации цифровых подписей, шифрование и т.д.

Учитывая повышение спроса на услуги электронной цифровой подписи на ЭК в коммерческих и государственных учреждениях, масштабы возможного ущерба при реализации атак на эллиптическую кривую постоянно возрастают.

Для практического использования ЭК международными и национальными стандартами предусмотрены процедуры генерации кривой, которые в определенной степени накладывают ограничения на время генерации параметров кривой. Учитывая тенденцию снижения криптографической стойкости алгоритмов с ростом вычислительных мощностей в мире, проблема генерации кривой становится более актуальной.

Одним из известных подходов в генерации ЭК является генерация изоморфных кривых, сохраняющих структуру группы точек при сдвиге их координат. При этом следует определить точное число изоморфизмов или хотя бы дать оценку этого числа. В существующих работах [1,2] данная задача решена с некоторыми неточностями, которые будут рассмотрены далее. В связи с этим, целью данной работы является уточнение существующих выражений, трансформирующих базовую кривую для частного случая канонической формы базовой кривой, а также получение граничных оценок мощности множества трансформаций.

Обзор существующих результатов

Вопросам определения параметров ЭК уделено немало внимания в работах [3,4,5,8]. В большей степени полученные улучшения были основаны также на выборе эллиптических кривых специального вида, что снижает время генерации параметров кривой с одной стороны, а с другой уменьшает множество допустимых кривых, что может в перспективе снизить стойкость криптосистемы. Альтернативным подходом в данной ситуации, с целью избегания ограничений на пространство кривых, закрепленных в современных стандартах, является трансформация базовой кривой с оценкой мощности множеств трансформаций ЭК в канонической форме.

Изложение основных результатов работы

Нормальной формой базовой кривой над полем F_p в обозначениях, принятых в [1-6], называется кривая вида:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,\ a_k \in F_p \tag{1}$$

Линейное изоморфное преобразование координат этой кривой задается формулами:

$$y = u^3\bar{y} + su^2\bar{x} + t,\ x = u^2\bar{x} + r,\ u \neq 0, u, r, s, t \in \{0,.., p-1\} \tag{2}$$

При произвольных параметрах *u*, *r*, *s*, *t* преобразования получаем кривую вида:

$$\bar{E}: \bar{y}^2 + \bar{a}_1\bar{x}\bar{y} + \bar{a}_3\bar{y} = \bar{x}^3 + \bar{a}_2\bar{x}^2 + \bar{a}_4\bar{x} + \bar{a}_6,\ \bar{a}_i \in F_p \tag{3}$$

Необходимо получить соотношения связывающие коэффициенты $\bar{a}_i$ изоморфной кривой $\bar{E}$ (3) с коэффициентами базовой кривой (1).

Входящие в (1) составляющие на основе формулы (2) равны:

$$y^2 = u^6\bar{y}^2 + s^2u^4\bar{x}^2 + t^2 + 2u^5s\bar{x}\bar{y} + 2u^3ty + 2u^2stx,$$
$$a_1xy = a_1(u^5\bar{x}\bar{y} + u^4s\bar{x}^2 + u^2t\bar{x} + u^3r\bar{y} + u^2sr\bar{x} + rt),$$
$$a_3y = a_3(u^3\bar{y} + u^2s\bar{x} + t),$$
$$x^3 = u^6\bar{x}^3 + 3u^4r\bar{x}^2 + 3u^2r^2\bar{x} + r^3,$$
$$a_2x^2 = a_2(u^4\bar{x}^2 + 2u^2r\bar{x} + r^2),$$
$$a_4x = a_4(u^2\bar{x} + r).$$

Приравнивая коэффициенты из (1) и (3), получим:

$$\begin{cases} u\bar{a}_1 = (a_1 + 2s)u^6, \\ u^3\bar{a}_3 = (a_3 + a_1r + 2t)u^6, \\ u^2\bar{a}_2 = (a_2 + 3r - a_1s - s^2)u^6, \\ u^4\bar{a}_4 = (a_4 - 3a_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st)u^6, \\ u^6\bar{a}_6 = (a_6 + a_4r + r^2a_2 + r^3 - ta_3 - rta_1 - t^2)u^6. \end{cases} \tag{4}$$

Теперь уравнение в координатах $\bar{x}, \bar{y}$ имеет вид:

$$u^6\bar{y}^2 + u^5(a_1 + 2s)\bar{x}\bar{y} + u^3(a_3 + a_1r + 2t)y = u^6\bar{x}^3 + u^4(a_2 + 3r - a_1s - s^2)\bar{x}^2 +$$
$$u^2(a_4 - 3a_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st)\bar{x} + (a_6 + a_4r + r^2a_2 + r^3 - ta_3 - rta_1 - t^2).$$

Заменой $\tilde{y} = u^3\bar{y}$, и $\tilde{x} = u^2\bar{x}$ это уравнение приводится к независимому от параметра u виду:

$$\tilde{y}^2 + (a_1 + 2s)\tilde{x}\tilde{y} + (a_3 + a_1 r + 2t)\tilde{y} = \tilde{x}^3 + (a_2 + 3r - a_1 s - s^2)\tilde{x}^2 +$$
$$(a_4 - 3a_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st)\tilde{x} + (a_6 + a_4 r + r^2 a_2 + r^3 - ta_3 - rta_1 - t^2).$$

Умножим это уравнение на u^6, тогда после замены $Y = \tilde{y}u^3$ и $X = \tilde{x}u^2$, получим новое уравнение:

$$Y^2 + \bar{a}_1 XY + \bar{a}_3 Y = X^3 + \bar{a}_2 X^2 + \bar{a}_4 X + \bar{a}_6,$$

где

$$\begin{cases} \bar{a}_1 = (a_1 + 2s)u, \\ \bar{a}_3 = (a_3 + a_1 r + 2t)u^3, \\ \bar{a}_2 = (a_2 + 3r - a_1 s - s^2)u^2, \\ \bar{a}_4 = (a_4 - 3a_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st)u^4, \\ \bar{a}_6 = (a_6 + a_4 r + r^2 a_2 + r^3 - ta_3 - rta_1 - t^2)u^6. \end{cases} \quad (5)$$

Уравнение в координатах X, Y тождественно уравнению (3) в координатах $\bar{x}, \bar{y}$, поэтому эти обозначения равноценны.

Подробный вывод выражений (5) нам потребовался в связи с ошибкой, допущенной в работе [2]. В равенствах (4), приведенных в [2], были упущены сомножители u^6 в правых частях. В итоге, сомножители u^i соответствующих коэффициентов оказались в левых частях равенств, а не в правых, как в равенствах (5). Следует, однако, признать, что эта ошибка не катастрофическая, т.к. при $u \neq 0$ в поле F_p, при $p \neq 2,3$ всегда существует обратный элемент $\gamma = u^{-1}$.

Для базового уравнения (1), записанного в канонической форме, имеем $a_1 = a_2 = a_3$, тогда равенства (5) упрощаются:

$$\begin{cases} \bar{a}_1 = 2su, \\ \bar{a}_3 = 2tu^3, \\ \bar{a}_2 = (3r - s^2)u^2, \\ \bar{a}_4 = (a_4 + 3r^2 - 2st)u^4, \\ \bar{a}_6 = (a_6 + a_4 r + r^3 - t^2)u^6. \end{cases} \quad (6)$$

Пусть γ_1 – число изоморфных кривых, полученных трансформацией из канонической формы в каноническую, при этом $\bar{a}_1 = \bar{a}_2 = \bar{a}_3 = 0$, и, следовательно, $s = r = t = 0$. Тогда $\bar{a}_4 = u^4 a_4, \bar{a}_6 = u^6 a_6$. Число γ_1 определяется объемом множества различных пар $\bar{a}_4, \bar{a}_6$, зависящих от значений a_4, a_6 и порядка элементов u^4, u^6 в мультипликативной группе F^*_p.

Например, при $p = 7$ порядок группы $\#F^*_7 = 6$. Элемент $u^6 = 1 \bmod 7$, элемент $u^3 = \pm 1 \bmod 7$, элемент $u^4 \in \{1,2,4\}$ при $u \neq 1$ имеет порядок 3. Это значит, что число изоморфизмов $\gamma_1 = 1$ при $a_4 = 0, a_6 \neq 0$ (нарушение последнего условия дает сингулярную

кривую), либо $\gamma_1 = 3$ при $a_4 \neq 1$. С ростом p число γ_1, естественно, растет. Так, при $p = 11$, $\#F^*_{11} = 10 = 2*5$, степени элементов u^4, u^6 четны, а сами элементы $u \neq 1$ имеют порядок 5. Число различных пар элементов u^4, u^6 также равно 5, поэтому $\gamma_1 = \frac{p-1}{2} = 5$, при $p = 11$. Можно заметить, чтопары элементов $(\pm u)^4, (\pm u)^6$ пробегают все значения квадратичных вычетов в мультипликативной группе F^*_p, поэтому для любого поля верхняя граница

$$\gamma_1 \leq \frac{p-1}{2}, \tag{7}$$

т.е. рост числа изоморфизмов в канонической форме кривой линейный с нарастанием *p*.

Из равенств (6) видно, что число изоморфизмов кривой *E* при ненулевых параметрах *r, s, t* резко возрастает. Здесь первые 3 параметра кривых линейно независимы с разделенными переменными *r, s* и *t,* что позволяет найти верхнюю границу числа изоморфизмов при трансформации из канонической формы в нормальную:

$$\gamma_2 \leq \frac{1}{2}(p-1)p^3. \tag{8}$$

Здесь величина γ_2 растет уже пропорционально 4-ой степени порядка *p* поля. Уже при $p = 7$ можно получить до $3*7^3 = 1029$ кривых.

Из (2) следует, что преобразование точки в точку изоморфной кривой имеет вычислительную сложность не более 5 умножений в конечном поле (и не более 4-х умножений для канонической формы). В то же время привлечение для задач криптографии изоморфных кривых в нормальной форме с оценкой (8) для числа изоморфизмов позволяет при фиксации этого числа приблизительно вчетверо сократить длину модуля поля и соответственно увеличить производительность вычислений.

Выводы

Таким образом, в результате проведенных исследований было получено уточнение приведенных в [2] выражений для коэффициентов изоморфных эллиптических кривых при трансформации из нормальной формы в нормальную. На их основе были получены новые результаты для оценки верхней границы количества изоморфных кривых, представленных в канонической форме. В частности, трансформация кривой из канонической формы в каноническую дает линейную зависимость (7) верхней границы числа изоморфизмов с ростом порядка *p* поля. Подобная же граница (8) при переходе от канонической формы в нормальную пропорциональна уже p^4. Это позволяет значительно увеличить мощность пространства изоморфных кривых в области криптографических приложений, либо сократить длину модуля поля. Полученные результаты позволяют избежать дополнительных ограничений на множество допустимых стандартными кривых при генерации параметров ЭК. Оценки (7), (8) могут быть полезны для расчета показателей стойкости криптографических алгоритмов на основе преобразований в группе точек ЭК.

Список литературы: 1.*Смарт Н.* Криптография // Н. Смарт / Перевод с английского С.А. Кулешова под редакцией С.К. Ландо. - Москва: Техносфера, 2005. - 528 С. ISBN 5-94836-043-1.2. *Husemöller D.* Elliptic Curves, Second Edition // Springer – 2002 / Dale Husemöller ; with appendices by Stefan Theisen, Otto Forster, and Ruth Lawrence. - p. cm. — (Graduate texts in mathematics; 111) Includes bibliographical references and index.ISBN 0-

387-95490-2 (alk. paper). 3. *Broker R.*Constructing elliptic curves of prime order / R.Broker, P. Stevenhagen – Contemporary Mathematics, 2008. – P. 1728, №463. 4. *Buchmann J.* Efficient Construction of Cryptographically Strong Elliptic Curves / J. Buchmann, H. Baier – Lecture Notes in Computer Science. — 2001.-Vol.2138. 5. *Koblitz N.*Primality of the number of points on an elliptic curve over a finite field / N. Koblitz – Pacific J. Math. 1988. - Vol. 131(1). - P. 157165. 6. *Konstantinou E.* On the Efficient Generation of Elliptic Curves over Prime Fields / E. Konstantinou, C. Stamatiou, C. Zaroliagis – Lecture Notes In Computer Science, 2002. – Vol. 2523. –P. 333–348. 7. *Schoof R.* Counting points on elliptic curves over finite fields / R. Schoof – J. Theorie des Nombres des Bordeaux. 1995. - Vol.7. - P. 219-254. 8. *Stein W.* A database of elliptic curves first report / W.A. Stein, M. Watkins – Lecture Notes in Comput. Sci. - 2002. - Vol. 2369. - P.267-275.