ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ТЕХНОЛОГИЙ ПЕРЕДАЧИ И ОБРАБОТКИ ИНФОРМАЦИИ И СИГНАЛОВ

УДК 681.3

ОКРУГЛЕНИЕ ЧИСЕЛ ПО МОДУЛЮ ПОЛЯ ЭЛЛИПТИЧЕСКОЙ КРИВОЙ ПРИ ВЫПОЛНЕНИИ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ В СИСТЕМЕ ОСТАТОЧНЫХ КЛАССОВ

Лавриненко А.Н., Червяков Н.И.

В статье предлагается решение проблемы определения модулярного вычета числа по модулю поля эллиптической кривой, вычисляемого для округления промежуточных результатов криптографических преобразований, выполняемых в системе остаточных классов.

Ключевые слова: эллиптические кривые, модулярная арифметика, криптография, системы криптографической защиты информации.

Введение. Постановка задачи

Использование модулярной арифметики и системы остаточных классов (СОК) – одно из наиболее перспективных направлений в области оптимизации времени выполнения сложных математических расчетов. Многие трудоемкие вычисления, которые раньше приходилось проводить в длинной арифметике естественным образом можно заменить на модулярные, за счет чего существенно сократится размерность операндов и уменьшится время их обработки. Среди прикладных областей для применения СОК особое место занимает защита информации с ее не теряющей актуальности проблемой повышения качества и скорости выполнения криптографических преобразований. Использование СОК в криптографии для распараллеливания криптографического вычислительного процесса связано с необходимостью разработки эффективного метода округления результатов промежуточных операций по модулю большого конечного поля F_p, в котором указанные операции должны выполняться.

Эллиптическая криптография и модулярная арифметика

В современном мире наиболее эффективными считаются криптосистемы, построенные на точках эллиптической кривой (ЭК). Это обусловлено тем, что ЭК обеспечивает максимально возможную надежность СКЗИ на один бит размера задачи. Сравнительная оценка надежности криптосистем при различной длине ключей представлена в работе [1]. На основе использования ЭК в криптографии разработан действующий в РФ ГОСТ Р 34.10-2012.

При использовании уравнения ЭК

$$E: y^2 = x^3 + ax + b(\mathrm{mod}p),\ a,b \in F_p \qquad (1)$$

над большим конечным полем F_p с дискриминантом $(4a^3 + 27b^2) \neq 0$ для реализации любого известного алгоритма криптографических преобразований (например, по схеме Эль-Гамаля) требуется выполнять операции сложения точек P и Q ЭК вида $R(x_3, y_3) = P(x_1, y_1) + Q(x_2, y_2)$, по общим формулам:

- при $P \neq \pm Q$

$$\begin{aligned} x_3 &= \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2, \\ y_3 &= -y_1 + \frac{y_2 - y_1}{x_2 - x_1}(x_1 - x_3). \end{aligned} \qquad (2а)$$

- при $P = Q$

$$\begin{aligned} x_3 &= \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - x_1 - x_2, \\ y_3 &= -y_1 + \frac{3x_1^2 + a}{2y_1}(x_1 - x_3). \end{aligned} \qquad (2б)$$

Поскольку при выполнении арифметических операций по формулам (2) над большим конечным полем F_p потребуется выполнение трудоемкой операции инверсии, то данный метод предлагается заменить альтернативными преобразованиями в проективной системе координат (X, Y, Z) по формулам:

- при $P \neq \pm Q$

$$\begin{cases} x_3 = v_7 v_{12}, \\ y_3 = v_6(v_{10} v_3 - v_{12}) - v_{11} v_1, \\ z_3 = v_{11} v_5, \end{cases} \qquad (3)$$

$$\text{где}\begin{cases} v_1 = y_1 z_2, \quad v_2 = y_2 z_1, \quad v_3 = x_1 z_2, \\ v_4 = x_2 z_1, \quad v_5 = z_1 z_2, \\ v_6 = v_2 - v_1, \quad v_7 = v_4 - v_3, \quad v_8 = v_4 + v_3, \\ v_9 = v_6^{\,2}, \quad v_{10} = v_7^{\,2}, \quad v_{11} = v_7^{\,3} = v_7 \cdot v_{10}, \\ v_{12} = v_9 \cdot v_5 - v_{10} \cdot v_8; \end{cases}$$

- при $P = Q$

$$\begin{cases} x_3 = 2v_{11}v_4 \\ y_3 = v_6(4v_7 - v_{11}) - 8v_2 v_8, \\ z_3 = 8v_9 \end{cases}$$

$$\text{где}\begin{cases} v_1 = x_1^{\,2}, v_2 = y_1^{\,2}, v_3 = z_1^{\,2}; \\ v_4 = y_1 z_1, v_5 = x_1 y_1; \\ v_6 = av_3 + 3v_1, v_7 = v_4 v_5, v_8 = v_4^{\,2}; \\ v_9 = v_4 v_8, v_{10} = v_6^{\,2}, v_{11} = v_{10} - 8v_7, \end{cases}$$

a – коэффициент из E в (1); $P(x_1, y_1, z_1)$, $Q(x_2, y_2, z_2)$, $R(x_3, y_3, z_3)$ – точки ЭК в проективной системе координат [2].

Вычисления по формулам (3) целесообразнее проводить в модулярной арифметике СОК. Для любых двух чисел a и b в СОК справедливо

$$a \circ b \equiv ((\alpha_1 \circ \beta_1) \bmod p_1, (\alpha_2 \circ \beta_2) \bmod p_2, \\ ..., (\alpha_n \circ \beta_n) \bmod p_n), \quad (4)$$

где $(\circ)$ – любая модульная операция («+», «–», «*» – все кроме деления), через α_i и β_i обозначены цифры СОК-представления чисел a и b по соответствующим модулям p_i системы, n – размерность СОК, $q = \prod_{i=1}^{n} p_i$ – диапазон вычислений выбранной СОК. Эффективность применения СОК для вычислений была показана в работе [3]. Таким образом, основные криптографические вычисления с помощью (3) сводятся к модулярным.

Проводя арифметические операции над координатами точек ЭК (1) по формулам (3), мы должны выполнять редукцию по модулю поля ЭК на каждом этапе промежуточных вычислений, так как в противном случае будет происходить переполнение динамического диапазона СОК q и искажение конечного результата. Как показано в работе [4] наиболее эффективной является редукция средствами СОК и предпочтительнее, чтобы модуль p поля ЭК (1) был большим простым числом.

Редукция методами СОК задача не из легких, однако нас интересуют только методы вычисления остатка от деления двух чисел в СОК, не связанные с реальной необходимостью выполнения процедуры деления.

Поскольку все промежуточные результаты криптографических вычислений не должны превышать p, то для того, чтобы в вычислениях по формулам (3) не происходило переполнение диапазона СОК при выполнении одной бинарной арифметической операции, необходимо обеспечить выполнение условия

$$q \geq p * (p - 1), \quad (5)$$

где q – диапазон СОК, p – модуль поля ЭК (1).

Поскольку модуль p в соответствии с ГОСТ Р 34.10-2012 должен быть большим простым числом, то использование методов расширения остаточного представления числа в СОК в конечном итоге окажется малоэффективным.

Для успешного выполнения модулярной редукции двух чисел в СОК нам потребуется разработать модулярный метод округления, позволяющий эффективно вычислять искомый остаток от деления.

Модулярный алгоритм округления двух чисел в СОК

Итак, нам необходимо вычислить модулярный остаток от деления числа $A = (a_1, a_2, ..., a_n)$, представленного в СОК с диапазоном q, по модулю поля р ЭК, где p и q удовлетворяют условию (5).

Воспользуемся тем обстоятельством, что модуль p поля ЭК (1) – большое простое число, заранее известное и взаимно простое со всеми модулями p_i выбранной СОК, где $q = \prod_{i=1}^{n} p_i, i = \overline{1..n}$ – ее диапазон; n – размерность. При этом модули p_i, которые также являются простыми числами, напротив, должны быть числами небольшой или относительно малой размерности, с тем чтобы выполнялось условие малой размерности компонент операндов по любому произвольно выбранному каналу СОК, и тем самым обеспечивалась высокая скорость обработки результатов промежуточных вычислений.

Будем считать, что промежуточный результат вычислений по формулам (3) записан в числе A. Разделив поразрядно A на p, получим

$$a = \frac{A}{p} = \frac{ps + t + kq}{p} = s + \frac{t + kq}{p}, \qquad (6)$$

где a – формальное частное от деления; $s = \lfloor A / p \rfloor$ – реальное частное от деления; t – искомый модулярный остаток; q – диапазон СОК; k – целое. Таким образом, $t + kq$ делится на p и

$$t + kq = p \quad \text{или} \quad t = p - kq. \qquad (7)$$

Поскольку искомый остаток t не должен превышать p, то без потери общности можно взять модулярный вычет от обеих частей (7):

$$t \equiv 1 - k|q|_p (\mathrm{mod} p). \qquad (8)$$

Ввиду того, что числа p и q заранее известны, то вычисление $|q|_p$ можно провести заблаговременно, и это не представляет серьезных проблем, даже ввиду большой размерности операндов. Кроме того, зная заранее соотношение чисел $|q|_p$ и p, можно предварительно рассчитать, какое количество интервалов длиной $|q|_p$ содержится в p, и использовать это для предотвращения выхода числа за границы p при вычислении произведения $k|q|_p$. Что касается величины k, то, как показано в работе [5], на базе теории рангов можно считать, что k – это разница в рангах числа pa и фактического делимого. Иными словами

$$k = r_A - r_{pa}. \qquad (9)$$

Очевидно, что для удобства дальнейших вычислений по формулам (3) все вычисления по формуле (8) необходимо вести в исходной СОК с диапазоном q. Процесс определения формального частного a состоит в выполнении операции поразрядного деления на p в СОК, что так же несложно организовать, учитывая, что p заранее известно, и поэтому получить представление p и p^{-1} в СОК можно заблаговременно, используя стандартные вычислительные средства.

Для окончательного раскрытия неопределенности в вопросе эффективного определения модулярного остатка в СОК согласно (8) следует подобрать эффективный метод определения ранга числа. Воспользуемся приближенным методом определения ранга числа в СОК, эффективность которого была теоретически и практически показана в работе [6]. Для этой цели в выбранной СОК следует заранее запастись вещественными константами $k_i = \frac{\left|Q_i^{-1}\right|_{p_i}}{p_i}$, где $Q_i = Q / p_i, i = \overline{1..n}$. Тогда, как показано в [8], получить ранг числа r_A можно, вычислив целую часть выражения $\sum_{i=1}^{n} k_i a_i$.

Поскольку нас интересует только вычисление ранга числа, то размерность хранимых констант k_i можно заранее ограничить, исходя из теоретических знаний о вычислительных погрешностях, возникающих при выполнении элементарных арифметических операций. Ввиду того, что в операции вычисления ранга числа используются умножение целого числа a_i на константу k_i и попарное сложение полученных произведений, а в конечном итоге должен получиться целочисленный результат, то достаточно в записи констант k_i в десятичной части числа оставлять столько разрядов, сколько содержится в соответствующем целочисленном p_i, плюс один-два дополнительных разряда, которые будут использоваться при округлении промежуточных результатов. Это существенно сократит размерность операндов при вычислении ранга числа и повысит скорость выполнения данной операции.

Выводы

Использование модулярной арифметики в эллиптической криптографии открывает новые горизонты для повышения скорости выполнения криптографических преобразований. Реализация механизма криптографических вычислений средствами СОК влечет необходимость разработки эффективного механизма редукции результатов промежуточных вычислений по модулю p поля ЭК. Очевидно, что редукцию двух чисел в СОК следует также выполнять средствами СОК, для того чтобы исходные данные, промежуточные вычисления и результат редукции были представлены в модулярной форме. Таким образом, удастся избежать дополнительных операций по переводу чисел в СОК и, следовательно, не нарушится общая математическая модель модулярных криптографических вычислений по формулам (3).

В работе представлен специализированный метод вычисления модулярного остатка в СОК по большому заранее известному модулю p. Указанный метод может быть обобщен для любого заранее известного и неизвестного модуля p. При этом, если этот модуль будет числом малой размерности, то предпочтительнее использовать метод расширения остаточного представления числа, показанный в [4; 7], а если число p достаточно большое, то эффективнее будет использовать метод на основе формулы (8).

Кроме того, метод расширения остаточного представления числа может понадобиться и в случае, если p будет составное, при условии, что в числе его сомножителей окажутся числа p_i. В общем же случае если p заранее неизвестно, то потребуется еще одна трудоемкая операция вычисления мультипликативной инверсии $\left|p^{-1}\right|_q$. Тем не менее предложенный метод в целом является универсальным.

Литература

1. STANDARDS FOR EFFICIENT CRYPTOGRAPHY, SEC 2: Recommended Elliptic Curve Domain Parameters // Certicom Research, September 20, 2000. – 51 p.
2. Mugino Saeki, Elliptic Curve Cryptosystems, School of Computer Science // McGill University, Montreal, February 1997. – 82 p.
3. Лавриненко А.Н., Червяков Н.И. Разработка программной модели модулярного вычислителя и оценка времени выполнения модульных и немодульных операций // Материалы I РНК «Проблемы математики и радиофизики в области информационной безопасности». Ставрополь: ИИЦ «Фабула», 2012. – С. 253-263.
4. Лавриненко А.Н., Червяков Н.И. Математическая модель эллиптической криптосистемы на основе системы остаточных классов. // Материалы II МНПК «Фундаментальная наука и технологии – перспективные разработки». Т. 2. М.: Academic, 2013. – С. 188-196.
5. Акушский И.Я., Юдицкий Д.И. Машинная арифметика в остаточных классах. М., Сов. радио, 1968 – 439 с.
6. Лавриненко А.Н., Червяков Н.И. Исследование точных и приближенных методов выполнения немодульных операций в СОК // Современное состояние и приоритеты развития фундаментальных и прикладных исследований в области физики, математики и компьютерных наук: Материалы 57-ой НМК «Университетская наука – региону». Ставрополь, ИИЦ «Фабула». Ч. 1, 2012. – С.118-122.
7. Лавриненко А.Н., Червяков Н.И. Исследование немодульных операций в системе остаточных классов // Научные ведомости БелГУ. Сер: История. Политология. Экономика. Информатика. Белгород: Изд-во БелГУ, №1 (120), вып. 21/1, 2012. – С.110-121.
8. Червяков Н.И. Методы, алгоритмы и техническая реализация основных проблемных операций, выполняемых в системе остаточных классов // ИКТ. Т.9, №4, 2011. – С. 4-12.

MODULAR ROUNDING NUMBERS BY THE ELLIPTIC CURVE FIELD'S MODULE DURING CRYPTOGRAPHIC TRANSFORMATIONS IN THE SYSTEM OF RESIDUAL CLASSES

Lavrinenko A.N., Chervyakov N.I.

This article offers a solution for the problem of defining number's modular reduction by the elliptic curve field's module, calculated for rounding intermediate results of cryptographic transformations in the system of residual classes.

Keywords: *elliptic curves, modular arithmetic, cryptography, systems of cryptographic protection information.*

Лавриненко Антон Николаевич, аспирант Кафедра прикладной математики и математического моделирования (ПММ) Северо-Кавказского федерального университета (СКФУ). Тел. (8-865) 277-56-26. E-mail: k-fmf-primath@stavsu.ru

Червяков Николай Иванович, д.т.н., профессор, Заслуженный деятель науки и техники РФ, заведующий Кафедрой ПММ СКФУ. Тел. (8-865) 275-35-64. E-mail: k-fmf-primath@stavsu.ru