

МЕТОД СЛОЖЕНИЯ ТОЧЕК ЭЛЛИПТИЧЕСКОЙ КРИВОЙ В ПРОЕКТИВНЫХ КООРДИНАТАХ ЛОПЕСА-ДАХАБА

В.Ю. Ковтун

(представил д.т.н., проф. Ю.В. Стасев)

В данной работе рассматривается новый метод сложения точек эллиптической кривой над двоичным полем в проективных координатах Лопеса-Дахаба.

Введение. Интенсивное развитие информационных технологий привело к их повсеместному применению. С каждым годом растет количество услуг доступных через глобальные сети, увеличиваются объемы циркулирующей в них информации, значительная доля которой является конфиденциальной или обладает некоторой ценностью. Глобальные сети находят широкое применение в финансово-кредитной сфере, и вскоре может фактически отпасть необходимость в наличных деньгах, большинство платежей станут электронными. Уже сегодня электронный денежный оборот в несколько раз перекрывает мировой товарооборот. Очевидно, что это приводит к возникновению угроз нанесения значительного урона, как частным, так и государственным организациям. Поэтому, чрезвычайную актуальность приобретают задачи обеспечения конфиденциальности, целостности, доступности, управления доступом, аутентификации, невозможности отращения и пр. Наиболее эффективным путем решения перечисленных выше задач является применение асимметричной криптографии.

Постановка задачи. В основу современных криптографических преобразований с открытым ключом положены преобразования в группе точек эллиптической кривой (ЭК) и в ряде стран они приняты в качестве криптографических стандартов [1 – 4]. Украина также является обладательницей такого стандарта, одной из важных областей применения которого, является банковская сфера. Увеличение количества вкладчиков и популярности удаленных средств управления банковскими счетами приводит к постоянному росту нагрузки на систему безопасности, что может привести даже к ее отказу. В этих условиях, одной из важных научно-технической задач является повышение быстродействия системы безопасности, и в частности криптопреобразований на ЭК. В качестве основной операции при криптопреобразованиях на ЭК выступает скалярное умножение [1 – 4], в основе

которого лежит сложение и удвоение ее точек [1 – 4, 6 – 9].

Целью настоящей работы является описание нового метода сложения точек ЭК в проективной системе координат Лопеса-Дахаба [7, 13], позволяющего уменьшить сложность.

Повышение производительности скалярного умножения можно достигнуть за счет увеличения скорости выполнения сложения и удвоения.

Будем рассматривать ЭК $E(\text{GF}(2^m))$, которая описывается усеченной формой уравнения Вейерштрасса [11 – 13]:

$$y^2 + xy = x^3 + ax^2 + b, \quad (1)$$

где $a, b \in \text{GF}(2^m)$ при $b \neq 0$.

Сложение точек в аффинных координатах. Напомним, сущность операции сложения точек ЭК в аффинных координатах, которая, как известно, основана на методе секущих Диофанта. Пусть E эллиптическая кривая, заданная уравнением (1) и $P_1(x_1, y_1)$, $P_2(x_2, y_2)$ точки кривой E , тогда результирующая точка $P_3(x_3, y_3) = P_1 + P_2$ вычисляется как:

$$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a; \quad (2)$$

$$y_3 = (x_1 + x_3)\lambda + x_3 + y_1, \quad (3)$$

где

$$\lambda = \frac{y_1 + y_2}{x_1 + x_2}, \text{ если } P_1 \neq P_2; \quad (4)$$

$$\lambda = \frac{y_1}{x_1} + x_1, \text{ если } P_1 = P_2. \quad (5)$$

Наиболее вычислительно сложной операцией является инверсия элемента поля [1 – 10]. Для того, что бы исключить эту операцию в (4) и (5), переходят к проективным координатам [1 – 5, 7 – 9].

Сложение точек в проективных координатах Лопеса-Дахаба. Наиболее вычислительно сложной операцией является инверсия элемента поля [1 – 10]. Для того, что бы исключить эту операцию в (4) и (5), переходят к проективным координатам [1 – 5, 7 – 9].

На сегодняшний день в литературе известно несколько видов проективных координат, наиболее эффективными проективными координатами для выполнения групповых операций на $E(\text{GF}(2^m))$, являются проективные координаты Лопеса-Дахаба [7, 9].

Поскольку предлагаемый здесь подход основан на использовании координат Лопеса-Дахаба, кратко изложим основные этапы этого метода сложения и удвоения точек.

Уравнение кривой в проективных координатах:

$$Y^2 + XYZ = X^3Z + aX^2Z^2 + bZ^4. \quad (7)$$

Для заданных точек $P_1(X_1, Y_1, Z_1)$, $P_2(X_2, Y_2, Z_2)$ кривой в проективном виде (7), координаты результирующей точки $P_3(X_3, Y_3, Z_3) = P_1 + P_2$, при P_1 не принадлежащие одному и тому же классу смежности с P_2 , определяются соотношениями:

$$X_3 = A^2 + I \cdot (D + a \cdot C^2) + A \cdot D; \quad (8)$$

$$Y_3 = Z_3 \cdot (X_3 + I \cdot E) + A \cdot B \cdot (F \cdot Z_3 + X_3 \cdot I); \quad (9)$$

$$Z_3 = D^2, \quad (10)$$

где $E = Y_2 \cdot Z_1^2$; $A = Y_1 \cdot Z_2^2 + E$; $F = X_1 \cdot Z_2$; $B = F + X_2 \cdot Z_1$; $C = Z_1 \cdot Z_2$; $D = B \cdot C$; $I = B^2$.

При P_1 и P_2 принадлежащим одному классу смежности, координаты результирующей точки $P_3(X_3, Y_3, Z_3)$, вычисляются по формулам:

$$X_3 = B^2 + A; \quad (11)$$

$$Y_3 = A \cdot Z_3 + X_3 \cdot (a \cdot Z_3 + Y_1^2 + A); \quad (12)$$

$$Z_3 = B \cdot C, \quad (13)$$

где $A = b \cdot C^2$; $B = X_1^2$; $C = Z_1^2$.

Отметим, что сложность операции сложения, согласно выражениям (8) – (10), операции удвоения, согласно выражениям (11) – (13), описывается соответственно соотношениями:

$$I_{\text{add}}(\text{LDPtj}) = 15I_{\text{mul}} + 6I_{\text{sqr}} + 8I_{\text{add}}; \quad (14)$$

$$I_{\text{dbl}}(\text{LDPtj}) = 5I_{\text{mul}} + 5I_{\text{sqr}} + 4I_{\text{add}}. \quad (15)$$

Предлагаемый подход. Идея развиваемого в работе подхода стоит в использовании, для перехода к проективным координатам Лопеса-Дахаба, дополнительных преобразований при вычислении x -координаты, позволивших уменьшить количество полевых операций. Изложим сущность этих преобразований.

Пусть даны точки $P_1(x_1, y_1)$, $P_2(x_2, y_2) \in E$, причем $P_1 \neq P_2$. Очевидны тождества:

$$y_1^2 + x_1y_1 \equiv x_1^3 + ax_1^2 + b; \quad (16)$$

$$y_2^2 + x_2y_2 \equiv x_2^3 + ax_2^2 + b. \quad (17)$$

Сложение тождеств (16) и (17) друг с другом дает

$$y_1^2 + y_2^2 + x_1y_1 + x_2y_2 \equiv x_1^3 + x_2^3 + ax_1^2 + ax_2^2. \quad (18)$$

Для вычисления x -координаты результирующей точки

$P_3(x_3, y_3) = P_1 + P_2$ из выражения (2) с учетом (4), последовательно получаем

$$\begin{aligned} x_3 &= \frac{(y_1 + y_2)^2}{(x_1 + x_2)^2} + \frac{(y_1 + y_2)}{(x_1 + x_2)} + x_1 + x_2 + a = \\ &= \frac{y_1^2 + y_2^2 + x_1 y_1 + x_1 y_2 + x_2 y_1 + x_2 y_2}{(x_1 + x_2)^2} + \\ &+ \frac{x_1^3 + x_2^3 + x_1^2 x_2 + x_1 x_2^2 + a x_1^2 + a x_2^2}{(x_1 + x_2)^2}. \end{aligned} \quad (19)$$

С учетом тождества (18), из (19) имеем

$$x_3 = \frac{x_1^2 x_2 + x_1 x_2^2 + x_1 y_2 + x_2 y_1}{(x_1 + x_2)^2}. \quad (20)$$

Полученный результат, выгодно отличается от известного [9], отсутствием параметра кривой a , что позволяет алгоритму сложения работать с различными эллиптическими кривыми с одинаковой производительностью и использовать один и тот же блок групповых операций для различных кривых.

Преобразуем выражения (20) и (3) для координат точки кривой к проективному виду. При переходе к координатам Лопеса-Дахаба [7, 9] аффинным точкам $P_1(x_1, y_1)$ и $P_2(x_2, y_2) \in E$ будут соответствовать точки $Q_1(X_1, Y_1, Z_1)$ и $Q_2(X_2, Y_2, Z_2)$, такие, что $x = X/Z$, $y = Y/Z^2$.

Подстановка новых переменных в выражения (20) и (3) позволяет представить проективные координаты в виде:

$$X_3 = X_2 Z_1 (Y_1 Z_2^2 + (X_1 Z_2)^2) + X_1 Z_2 (Y_2 Z_1^2 + (X_2 Z_1)^2); \quad (21)$$

$$\begin{aligned} Y_3 &= (X_1 Z_2 + X_2 Z_1) (Y_1 Z_2^2 + Y_2 Z_1^2) (X_1 Z_2 (X_1 Z_2 + X_2 Z_1)^2 + X_3) + \\ &+ Y_1 Z_2^2 (X_1 Z_2 + X_2 Z_1)^4 + Z_3 X_3; \end{aligned} \quad (22)$$

$$Z_3 = Z_1 Z_2 (X_1 Z_2 + X_2 Z_1)^2. \quad (23)$$

Обозначим $D = X_1 \cdot Z_2$; $E = X_2 \cdot Z_1$; $F = Y_1 \cdot Z_2^2$; $G = Y_2 \cdot Z_1^2$; $A = D + E$; $B = F + G$; $C = Z_1 \cdot Z_2$; $H = D^2$; $J = E^2$; $K = A^2 = H + J$. С учетом введенных обозначений, формулы (21), (22) преобразуются к виду:

$$X_3 = D \cdot (G + H) + E \cdot (F + J); \quad (24)$$

$$Y_3 = A \cdot B \cdot (K \cdot D + X_3) + (F \cdot K^2 + X_3 \cdot Z_3); \quad (25)$$

$$Z_3 = K \cdot C. \quad (26)$$

Сложность нового метода сложения получится равной

$$I_{\text{add}}(\text{LDPtj}^*) = 13I_{\text{mul}} + 5I_{\text{sqr}} + 9I_{\text{add}}. \quad (27)$$

Дополнительного повышения производительности можно добиться посредством использования смешанных координат [8]. В смешанных координатах рассмотрим точки $Q_1(X_1, Y_1, Z_1)$ и $Q_2(X_2, Y_2, 1)$. В этом случае выражения (24) – (26) упростятся:

$$X_3 = X_1 \cdot (G + H) + E \cdot (Y_1 + J); \quad (28)$$

$$Y_3 = A \cdot B \cdot (K \cdot X_1 + X_3) + (Y_1 \cdot K^2 + X_3 \cdot Z_3); \quad (29)$$

$$Z_3 = K \cdot Z_1, \quad (30)$$

где $E = X_2 \cdot Z_1$; $G = Y_2 \cdot Z_1^2$; $A = X_1 + E$; $B = Y_1 + G$; $H = X_1^2$; $J = E^2$; $K = A^2 = H + J$.

Сложность нового метода сложения в смешанных координатах:

$$I_{\text{add}}^{\text{mix}}(\text{LDPtj}^*) = 10I_{\text{mul}} + 4I_{\text{sqr}} + 9I_{\text{add}}. \quad (31)$$

В табл. 1 приведены результирующие оценки сложности выполнения арифметических операций на ЭК при использовании аффинных координат, координат Лопеса-Дахаба [9] и подхода развитого в работе (последняя строка таблицы). В таблице в столбце Σ^* обозначенная суммарная сложность методов относительно операции умножения в поле $\text{GF}(2^m)$.

Таблица 1

Сложность операций на эллиптической кривой

| Система координат | Общее сложение | | | | Общее сложение (смешанные координаты) | | | | Удвоение | | | |
|--|----------------|------------|----|------------|--|------------|----|------------|----------|------------|---|------------|
| | / | \wedge^2 | * | Σ^* | / | \wedge^2 | * | Σ^* | / | \wedge^2 | * | Σ^* |
| Аффинная, (x, y) | 1 | 1 | 2 | 12,6 | – | – | – | | 1 | 1 | 2 | 12,6 |
| Проективная Лопес-Дахаб, [9], $(x/z, y/z^2)$ | – | 6 | 15 | 15,7 | – | 4 | 10 | 10,4 | – | 5 | 5 | 5,55 |
| Проективная Лопес-Дахаб (новый подход), $(x/z, y/z^2)$ | – | 5 | 13 | 13,5 | – | 4 | 10 | 10,4 | | | – | |

Из данных приведенных в табл. 1 следует, что предлагаемый подход позволяет экономить 2 операции умножения.

Заключение. Полученный выигрыш в 2 операции, позволяет достичь повышения производительности классического алгоритма скалярного умножения на 8,94%, по сравнению с известными [9]. Внешне, выигрыш кажется незначительным, однако при выполнении большого количества операций скалярного умножения, эффект от его применения становится ощутимым. В качестве примера рассмотрим процессинговый центр банка

по работе с пластиковыми картами. Так, при выполнении банковских транзакций осуществляется верификация цифровых подписей, что требует выполнения скалярных умножений [1-3]. Использование предложенного подхода позволяет увеличить количество верификаций ЦП с 1 млн. до 1 млн. 89,4 тыс. транзакций, без дополнительных капиталовложений.

Дополнительным преимуществом полученных выражений, является независимость полученных выражений от параметров кривой.

ЛИТЕРАТУРА

1. ДСТУ 4541-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка.
2. IEEE P1363 / D9 (Draft Version 9). Standard Specifications for Public Key Cryptography, 1999.
3. AMERICAN NATIONAL STANDARD X9.62-1998 (Draft version), Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA).
4. Johnson D., Menezes A., Vanstone S. The elliptic curve digital signature. – Certicom research 2001. Canada. – 140 p.
5. Ковтун В.Ю., Смирнов О.А., Стасева Я.Ю. Представление точек эллиптической кривой над двоичными полями. // Системи обробки інформації. – Х.: НАНУ, ПАНМ, ХВУ. – 2002. – Вып. 6 (22). – С. 228 – 232.
6. Agnew, G. B., Mullin, R. C., Vanstone, S. A. On the development of a fast elliptic curve cryptosystem // Advances in Cryptology EuroCrypt'92.– P. 11 – 18.
7. Hankerson D., Lopez Hernandez J., Menezes A. Software implementation of elliptic curve cryptography over binary fields // Advances in Cryptology Crypto '99. – P. 37 – 46.
8. Cohen H., Miyaji A., Ono T. Efficient elliptic curve exponentiation using mixed coordinates.– 334 p.
9. Lopez J., Dahab R. Improved algorithms for elliptic curve arithmetic's in $GF(2^n)$ // Selected Areas in Cryptography – SAC'98, LNCS 1556. – 1999. – P. 201 – 212.
10. Збитнев С.И. Проективная геометрия – не все так гладко // Радиотехника: Всеукр. межвед. науч.-техн. сб. – 2002. – Вып. 126. – С. 32 – 38.
11. Шафаревич И.П. Основы алгебраической геометрии. – М.: Наука, 1972. – 568 с.
12. Соловьев Ю.П. Рациональные точки на эллиптических кривых. // Соросовский образовательный журнал. – 1997. – № 10. – С. 138 – 143.
13. Степанов С.А. Арифметика алгебраических кривых. – М.: Наука, 1999. – 224 с.

Поступила 29.11.2004

КОВТУН Владислав Юрьевич, адъюнкт ХУ ВС. В 2000 году закончил ХВУ. Область научных интересов – защита информации в автоматизированных системах управления и сетях.