УДК 681.1.3.06:519.248.681

В.В. Вишенько, здобувач
В.Ю. Ковтун, ад'юнкт
В.Я. Півнєв, к.т.н., ст. викл.
О.А. Смірнов, ад'юнкт
Харківський військовий університет

МОДИФІКОВАНИЙ АЛГОРИТМ СКАЛЯРНОГО ДОБУТКУ ТОЧОК ЕЛІПТИЧНОЇ КРИВОЇ НАД ДВІЙКОВИМИ ПОЛЯМИ

(Представлено д.т.н., проф. Стасєвим Ю.В.)

У статті розглядаються алгоритми скалярного добутку точок еліптичної кривої, що застосовуються у криптографічних перетвореннях. Проведено аналіз методів підвищення швидкодії розглянутих алгоритмів у афінних та проективних координатах Лопеса Дахаба. Запропоновано вирази для безпосереднього обчислення скалярних добутків на множники виду 4, 8, 16.

Інформація, яка циркулює в автоматизованих системах управління та комп'ютерних мережах на сучасному стані розвитку інформаційних технологій, потребує захисту. Одним із методів її захисту є криптографічні перетворення.

На сьогоднішній день, одними з перспективних криптографічних перетворень є перетворення в групі точок еліптичної кривої над простими та розширеними полями [1–3].

Еліптична крива над полем $GF(2^m)$ є множина рішень (x, y) рівняння [1]:

$$y^2 + xy = x^3 + ax^2 + b,$$

де $x,\ y,\ a,\ b \in GF(2^m)$.

Основною операцією у цьому виді перетворень є скалярний добуток точки на число. Так, існує досить велика кількість алгоритмів скалярного добутку точок еліптичної кривої [1, 2, 4]. Операція добутку та мультиплікативного інвертування у полі використовується досить інтенсивно при додаванні та подвоєнні точок на кривій (1)–(6).

Операція подвоєння точки $2P_1(x_1, y_1) = P_2(x_2, y_2)$ обчислюється згідно з виразами [2]:

$$x_2 = \lambda^2 + \lambda + a, \tag{1}$$

$$y_2 = (x_1 + x_2)\lambda + x_2 + y_1, \tag{2}$$

$$\lambda = \frac{y_1}{x_1} + x_1. \tag{3}$$

Операція додавання точок $P_3(x_3, y_3) = P_1(x_1, y_1) + P_2(x_2, y_2)$ обчислюється згідно з виразами:

$$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a, \tag{4}$$

$$y_3 = (x_1 + x_3)\lambda + x_3 + y_1, \tag{5}$$

$$\lambda = \frac{y_1 + y_2}{x_1 + x_2}. \tag{6}$$

В роботах [1, 3–5] розглядаються алгоритми, в яких пропонується зменшити кількість групових операцій за рахунок передобчислень, а також застосування NAF (non-adjacent form) подання скалярного множника для зменшення кількості нулів, що йдуть підряд.

В роботах [3, 5–7] пропонується використовувати різноманітні проективні координати, щоб запобігти інтенсивного застосування операції мультиплікативного інвертування.

Метою даної статті є підвищити ефективність реалізації алгоритму скалярного добутку точки кривої на число за рахунок передобчислень та застосування різних подань точок кривої.

Один з методів підвищення швидкодії є застосування аналітичних виразів для безпосереднього обчислення добутку на множники 4, 8, 16. Проведено порівняння швидкодії такого підходу в проективних та афінних координатах, що дає можливість зупинитися на тому чи іншому методі в залежності від особливостей системи, що проектується.

Так, з виразів (1)–(6) видно, що основними операціями під час додавання точок кривої є операції добутку та інвертування елементів поля $GF(2^m)$, тому підвищити швидкодію алгоритму скалярного добутку можливо за рахунок зменшення кількості операцій інвертування та добутку поліномів. Можливо уникнути операції інвертування за рахунок переходу у поданні точки еліптичної кривої з афінного на проективне [1–4].

У [2] показано, що час, необхідний для виконання однієї операції інвертування, відповідає приблизно 10 операціям добутку.

З робіт [1, 2, 4, 5] відомо, що в алгоритмах скалярного добутку приходиться виконувати досить багато разів подвоєння точки на кривій, причому подвоєння йдуть підряд. Зрозуміло, що заміна подвоєнь, що йдуть підряд, на одну операцію може зменшити кількість операцій інвертування, які виконуються при послідовному обчисленні. В таблиці 1 наведено аналітичні вирази для обчислення скалярних добутків на множники 4, 8, 16. Так, у стовпчиках 1, 2 автори пропонують аналітичні вирази, що були ними отримані. Кількість операцій у них значно відрізняються від аналогічних виразів для множника 16, які наведені у роботі [5]. Множник 16 – множник, що найбільш часто використовується у алгоритмах добутку [2].

Таблиця 1

Аналітичні вирази та їх складність в афінних та проективних координатах Лопеса Дахаба для обчислення скалярного добутку на множники 4, 8, 16

Аналітичні вирази		
Отримані авторами		[5]
$4P = 2^2P = (x_2, y_2)$	$4P = 2^2P = (X_2, Y_2, Z_2)$	$4P = 2^2P = (x_2, y_2)$
1	2	3
$x_2 = \frac{D^2 + T}{R^2} + a$ $y_2 = \frac{T \cdot x_2 + (B^2)^2}{R^2} + x_2$ $U = x^2$ $N = U + y$ $J = N \cdot x$ $B = N^2 + J + a \cdot U$ $E = J + U$ $D = B \cdot (B + E) + U^2 \cdot U$ $R = B \cdot U$ $T = D \cdot R$	$X_2 = D^2 + D \cdot T + a \cdot Z_2$ $Y_2 = D \cdot R \cdot X_2 + Z_2 \cdot (B^4 + X_2)$ $Z_2 = T^2$ $G = X^2$ $M = Z^2 \cdot G$ $N = G + Y$ $J = Z \cdot N \cdot X$ $B = N^2 + J + a \cdot M$ $D = B^2 + B \cdot (J + M) + M \cdot G^2$ $R = B \cdot G$ $T = Z^2 \cdot R$	$x_2 = \frac{\zeta^2 + (\delta \cdot \gamma) \cdot \zeta}{(\delta\gamma)^2} + a$ $y_2 = \frac{\zeta(\delta\gamma) \cdot x_2 + (\delta^2)^2}{(\delta\gamma)^2} + x_2$ $\gamma = x^2$ $\eta = \gamma + y$ $\delta = \eta^2 + \eta \cdot x + a \cdot \gamma$ $\xi = \eta x + \gamma$ $\zeta = \delta \cdot (\delta + \xi) + \gamma^2 \cdot \gamma$
Кількість операцій: * : 9 + : 10 $(\,)^2$: 7 $(\,)^{-1}$: 1	Кількість операцій: * : 12 + : 10 $(\,)^2$: 8 $(\,)^{-1}$: -	Кількість операцій: * : 9 + : 10 $(\,)^2$: 7 $(\,)^{-1}$: 1
$8P = 2^3P = (x_3, y_3)$	$8P = 2^3P = (X_3, Y_3, Z_3)$	$8P = 2^3P = (x_3, y_3)$
$x_3 = \frac{A^2 + P}{R^2} + a$ $y_3 = \frac{(V^2)^2 + Px_3}{R^2} + x_3$ $U = x^2$ $N = U + y$ $J = N \cdot x$ $B = N^2 + J + a \cdot U$ $E = J + U$ $D = B \cdot (B + E) + U^2 \cdot U$ $T = B \cdot U$	$X_3 = O^2 + L + a \cdot Z_3$ $Y_3 = Z_3 \cdot (V^4 + X_3) + L \cdot X_3$ $Z_3 = H^2$ $G = X^2$ $N = G + Y$ $J = N \cdot X \cdot Z$ $M = Z^2 \cdot G$ $B = N^2 + J + a \cdot M$ $T = B \cdot G$ $F = Z^2 \cdot T$,	$x_3 = \frac{\omega^2 + \omega \cdot \rho}{\rho^2} + a$ $y_3 = \frac{(\upsilon^2)^2 + \omega\rho \cdot x_3}{\rho^2} + x_3$ $\gamma = x^2$ $\eta = \gamma + y$ $\xi = \eta \cdot x + \gamma$ $\delta = \eta^2 + \eta x + a \cdot \gamma$ $\zeta = \delta \cdot (\delta + \xi) + \gamma^2 \cdot \gamma$ $\upsilon = \zeta^2 + \tau \cdot \zeta + \tau^2 \cdot a$

Закінчення табл. 1

1	2	3
$S = D \cdot T$ $V = D^2 + S + T^2 \cdot a$ $R = VT^2$ $A = V(V + S) + T^2(B^2)^2 + R$ $P = AR$	$D = B^2 + B \cdot (J + M)$ $V = D^2 + F \cdot D + a \cdot F^2$ $O = V^2 + V \cdot F \cdot J + F^2 \cdot B^4$ $R = V \cdot T^2$ $H = Z^4 \cdot R$ $L = O \cdot H$	$\tau = \delta \cdot \gamma$ $\rho = \upsilon \cdot \tau^2$ $\omega = \upsilon \cdot (\upsilon + \zeta \cdot \tau) + (\tau \cdot \delta^2)^2 + \rho$
Кількість операцій: * : 14 + : 15 ( )^2 : 11 ( )$^{-1}$: 1	Кількість операцій: * : 18 + : 15 ( )^2 : 13 ( )$^{-1}$: -	Кількість операцій: * : 14 + : 15 ( )^2 : 11 ( )$^{-1}$: 1
$16P = 2^4 P = (x_4, y_4)$	$16P = 2^4 P = (X_4, Y_4, Z_4)$	$16P = 2^4 P = (x_4, y_4)$
$x_4 = \frac{F^2 + P}{L^2} + a$ $y_4 = \frac{(M^2)^2 + P \cdot x_4}{L^2} + x_4$ $U = x^2$ $N = U + y$ $J = N \cdot x$ $B = N^2 + J + a \cdot U$ $E = J + U$ $D = B^2 + B \cdot E + U^2 \cdot U$ $T = B \cdot U$ $S = D \cdot T$ $V = D^2 + S + T^2 \cdot a$ $R = V \cdot T^2$ $A = V^2 + V \cdot S + T^2 \cdot (B^2)^2 +$ $G = A \cdot R$ $M = A^2 + G + a \cdot R^2$ $L = M \cdot R^2$ $F = M^2 + M \cdot G + L + (V^2)^2 \cdot$ $P = L \cdot F$	$X_4 = F^2 + O + a \cdot Z_4$ $Y_4 = Z_4 \cdot (M^4 + X_4) + O \cdot X_4$ $Z_4 = P^2$ $G = X^2$ $N = G + Y$ $J = N \cdot X \cdot Z$ $Q = Z^2 \cdot G$ $B = N^2 + J + a \cdot Q$ $D = B^2 + B \cdot (J + Q) + Q \cdot G^2$ $T = B \cdot G$ $K = Z^2 \cdot T$ $L = D \cdot K$ $V = D^2 + L + a \cdot K^2$ $R = V \cdot T^2$ $U = Z^4 \cdot R$ $A = V^2 + V \cdot L + K^2 \cdot B^4 + U$ $I = A \cdot U$ $M = A^2 + I + a \cdot U^2$ $P = U^2 \cdot M$ $F = M^2 + I \cdot M + U^2 \cdot V^4 + P$ $O = F \cdot P$	$x_4 = \frac{\theta^2 + \theta \cdot \mu \cdot \rho^2}{(\mu\rho^2)^2} + a$ $y_4 = \frac{(\mu^2)^2 + (\theta\mu\rho^2) \cdot x_4}{(\mu\rho^2)^2} + x_4$ $\gamma = x^2$ $\eta = \gamma + y$ $\xi = \eta \cdot x + \gamma$ $\delta = \eta^2 + \eta x + a \cdot \gamma$ $\zeta = \delta \cdot (\delta + \xi) + \gamma^2 \cdot \gamma$ $\upsilon = \zeta^2 + \tau \cdot \zeta + \tau^2 \cdot a$ $\tau = \delta \cdot \gamma$ $\rho = \upsilon \cdot \tau^2$ $\omega = \upsilon \cdot (\upsilon + \zeta \cdot \tau) + (\tau \cdot \delta^2)^2 + \rho$ $\mu = \omega^2 \cdot \omega + \omega \cdot \rho + a \cdot \upsilon^2$ $\theta = \mu^2 + \mu \cdot (\omega\rho) + \mu\rho^2 \cdot \rho + (\upsilon^2 \cdot$
Кількість операцій. * : 19 + : 16 ( )^2 : 15 ( )$^{-1}$: 1	Кількість операцій: * : 23 + : 20 ( )^2 : 18 ( )$^{-1}$: -	Кількість операцій: * : 22 + : 20 ( )^2 : 16 ( )$^{-1}$: 1

Складність обчислення отриманих авторами виразів наведено у таблиці 2 для послідовного та безпосереднього обчислення як в афінних, так і в проективних координатах Лопеса Дахаба [3, 5, 7]. Для отримання виразів у проективних координатах автори користувалися виразами для подвоєння точок, що наведено у роботі [7]. Аргументи щодо вибору саме проективних координат Лопеса Дахаба наведено у роботі [7].

Проведемо аналіз ефективності наведених в таблиці перетворень відносно послідовного обчислення у афінних координатах, піднятого за допомогою сірого кольору. Тобто складемо рівняння кількості операцій кожного з перетворень та кількості операцій у афінних координатах для послідовного обчислення, результати подамо у таблиці 2.

Таблиця 2

Складність обчислення 4P, 8P, 16P в афінних координатах та проективних координатах Лопеса Дахаба

Операція	Координати	Складність				Відповідність кількості операцій A_{II}
		$(\ )^2$	*	+	$(\ )^{-1}$	
2P	A_{II}	2	2	5	1	
	$ЛД_{II}$	5	5	4	-	A_{II} (1In+1Ad) ↔ 3M+3S
4P	A_{II}	4	4	10	2	
	$A_{Б}$	7	9	10	1	A_{II} (1In) ↔ 5M+3S
	$ЛД_{Б}$	8	12	10	-	A_{II} (1In) ↔ 4M+2S
	$ЛД_{II}$	10	10	8	-	A_{II} (1In+1Ad) ↔ 3M+3S
8P	A_{II}	6	6	15	3	
	$A_{Б}$	11	14	15	1	A_{II} (1In) ↔ 4M+2,5S
	$ЛД_{Б}$	13	18	15	-	A_{II} (1In) ↔ 4,7M+2,3S
	$ЛД_{II}$	15	15	12	-	A_{II} (1In+1Ad) ↔ 3M÷3S
16P	A_{II}	8	8	20	4	
	$A_{Б}$	15	19	16	1	A_{II} (1In+1,3Ad) ↔ 3,7M+2,3S
	$ЛД_{Б}$	18	23	20	-	A_{II} (1In) ↔ 3,75M+2,5S
	$ЛД_{II}$	20	20	16	-	A_{II} (1In) ↔ 3M+3S

де A – афінні координати;

$ЛД$ – проективні координати Лопеса Дахаба $\left(\frac{X}{Z};\frac{Y}{Z^2}\right)$;

$(\ )_{II}$ – послідовний метод обчислення;

$(\ )_{Б}$ – безпосередній метод обчислення;

In – операція інвертування;

M – операція добутку;

S – операція піднесення до квадрата;

Ad – операція додавання.

Наведемо алгоритми [3], де можливе застосування отриманих авторами виразів.

В алгоритмі 1 для різної ширини вікна передобчислень застосовуються вирази з таблиці 2 для безпосереднього обчислення добутку $2^t P$, де $d = \lceil (t-1)/w \rceil$.

Алгоритм 1. Двійковий алгоритм обчислення скалярного добутку з шириною вікна передобчислень $w = 4$.

Вхід: $k = (k_{t-1},\ldots,k_1,k_0)_2$, $P \in E(F_{2^m})$, w – ширина вікна передобчислень.

Вихід: kP.

1. Передобчислення $C[(k_{i+(w-1)},\ldots,k_{i+1},k_i)]$, для всіх можливих комбінацій $(k_{i+(w-1)},\ldots,k_{i+1},k_i)$, де $(k_{i+(w-1)},\ldots,k_{i+1},k_i)$ – біти скалярного множника k, що йдуть підряд. При досить великій ширині вікна передобчислень $C[(k_{i+(w-1)},\ldots,k_{i+1},k_i)]$ – обчислюються по мірі необхідності.

2. $Q = 0$.

3. $d = \lceil (t-1)/w \rceil$.

4. For i from $d-1$ downto 0 do

   3.1. $Q = 2^w \cdot Q$.

   3.2. $Q = Q + C[(k_{i+(w-1)},\ldots,k_{i+1},k_i)]$.

5. Return (Q).

Алгоритм 1 має складність за часом:

$$T_1 = \left[(2^w - 1)\cdot A\right]_{передобчислення} + \left[(d-1)\cdot A + (d-1)\cdot w \cdot D\right]_{обчислення}, \qquad (7)$$

де A – час виконання операцій додавання двох точок;

D – час виконання операції подвоєння точки.

Аналітичні вирази, отримані авторами, дозволяють зменшити час виконання операції скалярного добутку на етапі обчислень. Зрозуміло, що на етапі безпосередніх обчислень множник w означає, що необхідно виконати w подвоєнь, які можливо замінити на безпосереднє обчислення, згідно з виразами, отриманими авторами для скалярних множників 4, 8, 16, що наведені у стовпчиках 1, 2 таблиці 1 для різних подань точок кривої.

В алгоритмі 2 на етапі передобчислень застосовуються вирази з таблиці 1 для безпосереднього обчислення добутків $2^{id}P$, $i = \overline{1, w}$. Так

$$C[k_{d(w-1)},...,k_d,k_0] = 2^{k_{d(w-1)}}P + ... + 2^{k_d}P + 2^{k_0}P, \quad (8)$$

де $d = \lceil (t-1)/w \rceil$, необхідно обчислити для всіх можливих комбінацій $(k_{d(w-1)},...,k_d,k_0)$, тобто 2^w можливих варіанти.

Алгоритм 2. Двійковий комбінований алгоритм обчислення скалярного добутку з шириною вікна передобчислень $w = 4$.

Вхід: $k = (k_{t-1},...,k_1,k_0)_2$, $P \in E(F_{2^m})$, w – ширина вікна передобчислень.

Вихід: kP.

1. Передобчислення $C[(k_{d(w-1)+i},...,k_{d+i},k_i)]$, для всіх можливих комбінацій $(k_{d(w-1)+i},...,k_{d+i},k_i)$, де $(k_{d(w-1)+i},...,k_{d+i},k_i)$ – біти k, що йдуть через кожні w бітів. При досить великій ширині вікна передобчислень $C[(k_{d(w-1)+i},...,k_{d+i},k_i)]$ – обчислюються по мірі необхідності.

2. $Q = 0$.

3. $d = \lceil (t-1)/w \rceil$.

4. For i from $d-1$ downto 0 do

   3.1. $Q = 2 \cdot Q$.

   3.2. $Q = Q + C[(k_{d(w-1)+i},...,k_{d+i},k_i)]$.

5. Return (Q).

Алгоритм 2 має складність за часом:

$$T_2 = \left[\frac{(2^w - 1)}{2} \cdot A + d \cdot (w-1) \cdot D \right]_{передобчислення} + \left[(d-1) \cdot A + (d-1) \cdot D \right]_{обчислень}, \quad (9)$$

де A – час виконання операцій додавання двох точок; D – час виконання операції подвоєння точки.

Аналітичні вирази, отримані авторами, дозволяють зменшити час виконання операції скалярного добутку на етапі передобчислень. Так, для виконання множення точок на множники 2^w та 2^d.

На підставі результатів, наведених у таблиці 2, можна констатувати наступне:

1. Використання виразів, стовпчик 1 таблиці 1, дозволяє значно зменшити число операцій інвертування в полі, відносно послідовного обчислення, а також потребує меншу кількість операцій відносно результатів роботи [5].

2. Використання виразів, стовпчик 1 таблиці 1, доцільне, якщо неможливо використовувати проективні координати Лопеса Дахаба та час виконання однієї операції інвертування перевищує час виконання 3, 7 операцій добутку.

3. Використання проективних координат доцільне у випадку, коли час виконання операції інвертування перевищує час виконання 3 операцій добутку. В координатах ЛД при послідовному застосуванні подвоєння маємо меншу кількість операцій множення, що приходяться на одну операцію інвертування в полі відносно безпосереднього. Застосування виразів для обчислення *4P, 8P, 16P* у координатах *ЛД* – недоцільне, бо кількість операцій добутку для послідовного обчислення відносно безпосереднього – значно менше.

Щодо застосування алгоритмів 1 та 2. У випадку, коли час перетворення – критичний і перетворення застосовується для великої кількості даних, бажано користуватися алгоритмом 2. У ньому значний час займають передобчислення, а безпосередні обчислення – незначний. У

випадку, коли час критичний і перетворення застосовується для невеликої кількості даних, бажано користуватися алгоритмом 1. У ньому значний час тратиться на безпосередні обчислення, а незначний – на передобчислення.

В подальшому для підвищення швидкодії криптографічних перетворень в групі точок еліптичної кривої пропонується перехід до еліптичних кривих спеціального вигляду.

ЛІТЕРАТУРА:

1. IEEE P1363 / D9 (Draft Version 9). Standard Specifications for Public Key Cryptography, 1999.

2. *Hankerson D., Hernandez J.L., Menezes A.*. Software implementation of elliptic curve cryptography over binary fields. Advances in Cryptology Crypto '99.

3. *Milne J.S.* Elliptic curves. . University of Michigan? 1996.

4. *Smart N.P., Westwood E.J.* Point Multiplication on Ordinary Elliptic Curves over Fields of Characteristic Three. Computer Sciences Department University of Bristol. United Kingdom.

5. *Guardo J., Paar C.* Efficient algorithms for elliptic Curve Cryptosystems. ECE Department, Worcester Polytechnic Institute, Worcester, MA 01609, USA.

6. *Збитнев С.И.* Проективная геометрия – не все так гладко // Радиотехника: Всеукр. межвед. науч.-техн. сб. – 2002. – Вып. 126. – С. 78–85.

7. *Ковтун В.Ю., Смирнов А.А., Стасева Я.Ю.* Представление точек эллиптической кривой над двоичными полями // Системи обробки інформації. – Харків: НАНУ, ПАПМ, ХВУ, 2002. – Вып. 6(22). – С. 24–28.

ВИШЕНЬКО Владлена Володимирівна – здобувач Харківського військового університету.
Наукові інтереси:
– захист інформації в автоматизованих системах та мережах;
– побудова розподілених обчислювальних систем.
E-mail: vishvlvl@mail.ru

КОВТУН Владислав Юрійович – ад'юнкт Харківського військового університету.
Наукові інтереси:
– захист інформації в автоматизованих системах та мережах.
Тел.: (0572) 40-28-07.
E-mail: vjet@mail.ru

ПЄВНЄВ Володимир Якович – кандидат технічних наук, доцент, старший викладач кафедри Харківського військового університету.
Наукові інтереси:
– оптимізаційні задачі на графах;
– системи захисту інформації та їх криптоаналіз.
Тел.: (0572) 40-28-33.
E-mail: pevnev@kpi.kharkov.ua

СМІРНОВ Олексій Анатолійович – ад'юнкт Харківського військового університету.
Наукові інтереси:
– захист інформації в автоматизованих системах та мережах.
Тел.: (0572) 40-28-33.

Подано 20.07.2003