УДК 004.056

Р. С. Ганзя, аспірант
Харківський національний університет радіоелектроніки, м. Харків

МОДИФІКОВАНИЙ МЕТОД ОБЧИСЛЕННЯ ПОРЯДКУ ЕЛІПТИЧНИХ КРИВИХ

Наведений модифікований алгоритм обчислення порядку еліптичної кривої, визначеної над двійковим полем. Порівнюються теоретичні та експериментальні показники обчислювальної складності даного метода та його базової версії. Робляться висновки щодо можливості його використання для модифікації національних стандартів.

Ключові слова: *порядок еліптичної кривої, метод SST, метод MSST.*

Вступ. Останнім часом стає актуальним питання підвищення рівня стійкості асиметричних криптоперетворень. Основними причинами необхідності підвищення рівня стійкості є: швидкий розвиток квантових технологій та існування квантового криптоаналізу, прийняття нових національних стандартів (симетричного шифру та геш-функції) з надвисоким рівнем стійкості, обмеження в загальних параметрів в національному стандарті електронного цифрового підпису (до 431 біта).

У зв'язку з цим існує необхідність розробки теоретичного та практичного фундаменту генерування загальних параметрів асиметричних криптоперетворень для полів характеристики два (як в національному стандарті). Основною задачею при формування параметрів є задача обчислення порядку еліптичної кривої. Далі в роботі буде наведено алгоритм, що дозволяє за поліноміальний час вирішити задачу швидкого обчислення порядку кривої.

У роботі [1] Гаудрі запропонував поєднати ідею арифметико-геометричного методу та методу Сато, Ск'єрна та Тагучі. Детально метод AGM був нами проаналізований у роботі [2]. Варто звернути увагу, що для роботи MSST слід використовувати однозмінну варіацію методу AGM, хоча з точки зору обчислювальної складності однозмінний та двозмінний AGM майже не відрізняються. Проте використання однозмінного передбачає використання AGM-послідовності $(a_k, b_k)_{k=0}^{\infty}$ в якій $a_k \equiv b_k \equiv 1 \bmod 4$ та $a_k \equiv b_k \bmod 8$ у наступному варіанті $\lambda_k \equiv a_k / b_k$, що відповідає еліптичній кривій:

$$E_{\lambda_k} : y^2 = x(x-1)(x-\lambda_k^2)\,. \qquad (1)$$

Так як кожна попередня AGM-послідовність дає можливість обчислювати наступну, тобто така послідовність є ітеративною

$(a_{k+1}, b_{k+1}) = ((a_k + b_k)/2, \sqrt{a_k b_k})$, ми можемо представити ітеративну функцію однозмінної AGM-послідовності у вигляді $\lambda_{k+1} = \frac{2\sqrt{\lambda_k}}{1+\lambda_k}$ [12].

Ініціалізація однозмінної AGM-послідовності здійснюється наступним чином:

$$\lambda_1 \equiv (1+8c) \bmod 16, \tag{2}$$

де $c \equiv \bar{c} \bmod 2$ є вільним коефіцієнтом еліптичної кривої. Гаудрі також доводить що послідовність λ_{k+1} сходиться так само як і a_k / b_k, мається на увазі, що $\lambda_{k+1} \equiv \sum(\lambda_k) \bmod 2^{k+3}$ і якщо підставити дане значення у значення ітеративної функції AGM-послідовності отримаємо:

$$\sum(\lambda_k)^2 (1+\lambda_k)^2 - 4\lambda_k \equiv 0 \bmod 2^{k+3}. \tag{3}$$

Вищенаведений вираз вирішується з використанням головної ідеї алгоритма SST [3]. Гаудрі представляє вирішення цієї проблеми через зміну виразу модулярного полінома, що використовується для підняття еліптичної кривої.

Нехай $E(X,Y)$ буде модульним виразом AGM, тоді:

$$E(X,Y) = Y^2(1+X)^2 - 4X = 0. \tag{4}$$

Наведене вище представлення дозволяє використати умову модулярних поліномів (теорема Любліна Сьерра та Тейта) у вигляді $E_2(X, \sum(X)) \equiv 0 \bmod 2^{k+3}$. Слід зазначити, що обидві часткові похідні дорівнюють нулю по модулю 2 у цьому виразі, тому ми не можемо безпосередньо використовувати алгоритм SST. Для усунення такої проблеми Гаудрі пропонує наступні заміни $X \leftarrow 1+8X$, а $Y \leftarrow 1+8Y$ і в результаті отримаємо модифікований модулярний поліном для полів характеристики два у вигляді:

$$\tilde{E} = (X + 2Y + 8XY)^2 + Y + 4XY = 0, \tag{5}$$

що може бути вирішеним, коли відомо X і він не дорівнює нуль по модулю два, так коли $Y = \sum(X)$. В такому випадку часткові похідні дорівнюють:

$$\begin{aligned} \frac{\partial \tilde{E}}{\partial X}(X,Y) &= 2(X + 2Y + 8XY)(1+8Y) + 4Y, \\ \frac{\partial \tilde{E}}{\partial Y}(X,Y) &= (4(X + 2Y + 8XY) + 1)(1+4X), \end{aligned} \tag{6}$$

не важко переконатися, що і справді кожна часткова похідна за X дорівнює нулю за модулем два, а за Y дорівнює одиниці, що задовольняє вимогам SST алгоритму [4].

Останнє, що необхідно зробити — це узгодити вираз з якого обчислюється слід Фробеніуса, для двозмінної AGM послідовності він виглядає наступним чином:

$$Tr\overline{F} = t_k + q / t_k \bmod^{k+3}, \tag{7}$$

з $t_k = N_{Q_q/Q_p}(a_k / a_{k+1})$, підставивши в цей вираз значення, що приймалися для однозмінного AGM, тобто $\lambda_k \equiv a_k / b_k$, $a_{k+1} = (a_k + b_k)/2$ та $\lambda_1 \equiv 1 + 8c$ отримаємо:

$$t_k = N_{Q_q/Q_p}\left(\frac{1}{1+4\lambda_k}\right). \tag{8}$$

Якщо поєднати алгоритм SST та ідею Гаудрі можна визначити наступний алгоритм, що запропонований автором у [1]:

Вхід: Еліптична крива $E: y^2 + xy = x^3 + \overline{c}$ над F_{2^d}

Вихід: Кількість точок кривої $E(F_{2^d})$

1. $N = \left\lceil \frac{d}{2} \right\rceil + 2;$
2. $y \equiv j \bmod 2;$
3. $m(x) = GenTeichmullerModule(f(x));$
4. $C = GenC_1(x) \bmod 2^N;$
5. *for* $i = 2$ *to* W *do*
   - 5.1 $x \equiv \Sigma^{-1}(y) \bmod 2^i;$
   - 5.2 $y \equiv y - \tilde{E}_2(x,y) \bmod 2^i;$
6. $x \equiv \Sigma^{-1}(y) \bmod 2^W;$
7. $D_x \equiv \frac{\partial \tilde{E}_2}{\partial X}(x,y) \bmod 2^W;$
8. $D_y \equiv \frac{\partial \tilde{E}_2}{\partial Y}(x,y) \bmod 2^W;$
9. *for* $m = 1$ *to* $\lfloor (N-1)/W \rfloor$ *do*
   - 9.1. $x \equiv \Sigma^{-1}(y) \bmod 2^{(m+1)W};$
   - 9.2. $V \equiv \tilde{E}_2(x,y) \bmod 2^{(m+1)W};$
   - 9.3. *for* $i = 0$ *to* $W - 1$ *do*
     - 9.3.1. $\Delta y \equiv -2^{-(mW+i)} V \bmod 2;$

9.3.2. $\Delta x \equiv \Sigma^{-1}(\Delta y) \mod 2^{W-i}$;

9.3.3. $y \equiv y + 2^{mW+i}\Delta y \bmod 2^{(m+1)W}$;

9.3.4. $V \equiv V + 2^{mW+i}(D_x\Delta x + D_y\Delta y) \bmod 2^{(m+1)W}$;

10. $t = Norm\left(\frac{1}{1+4y}\right) \bmod 2^N$;

11. *if* $t^2 > 2^{d+2}$ *then* $t \leftarrow t - 2^N$;

12. *return* $2^d + 1 - t$.

Після подання метода SST вищенаведений алгоритм не потребує особливих пояснень. Якщо порівняти два схожих метода SST та MSST з точки зору обчислювальної складності, то MSST звичайно працює швидше і для $W \approx n^{\mu/(1+\mu)}$ та $N \approx n/2$ його складність дорівнює $O(n^{2\mu+0,5})$. Викликано це передусім тим, що модулярний поліном, використаний в MSST потребує 1 множення та 1 підняття в квадрат, а в SST — 3 множення та 2 підняття в квадрат (мається на увазі в кільці p-адичних чисел). З точки зору просторової складності два методи потребують однакових ресурсів, просторова складність $O(n^2)$, хоча все ж таки константи, що використовуються в модулярному поліномі MSST значно менші, ніж ті що у SST. Фаза передобчислень для двох алгоритмів однакова і потребує $O(n^{2\mu+1})$ обчислювальних ресурсів для свого виконання [4].

Вище наведена теоретична оцінка складності фази підняття еліптичної кривої для SST та MSST, складність обчислення норми для одного з існуючих алгоритмів, що використовувався для обчислення порядку еліптичної кривої.

Для канонічного підйому було використано метод SST [3], метод MSST [1]). Для аналітичний метод (запропонований Сато, Ск'єрною та Тагучі) [3].

Для виконання обчислень кількості точок на еліптичній кривій було розроблено програмний засіб на мові C++ з використанням бібліотеки NTL та gmp. Дослідження, щодо часу виконання алгоритму проводилися на програмі, що була скомпільована з використанням gcc 4.84 на операційний системі Ubuntu 14.04 та процесорі Intrel Core i5-2300. Так як всі операції для такого класу алгоритмів виконуються послідовно, то розпаралелити виконання алгоритму неможливо, а кількість ядер у процесорі час виконання алгоритму не змінять.

У таблиці наведено час обчислення фази підйому для SST, MSST та норми. За результатами аналізу таблиці можна стверджувати, що спостерігається виграш метода MSST над його стандартною

модифікацією у SST, наші практичні результати підтверджують теоретичні дослідження даних методів.

Таблиця

Обчислювальна складність SST та MSST

Степінь розширення поля *d*, *біт*	**Фаза підйому**		**Нормування за SST, *с***
	SST, *с*	**MSST, *с***	
7	0,006265	0,003216	0,000248
23	0,023238	0,010162	0,00088
107	0,251051	0,123306	0,010746
173	0,680349	0,400715	0,028311
199	0,822255	0,501402	0,035182
257	0,950504	0,698594	0,054191
307	1,55134	1,17776	0,088748
383	2,39215	1,91847	0,133243
503	3,97648	3,2511	0,198481
601	7,15564	6,00326	0,424093
709	10,44	9,02212	0,532264
787	13,2826	11,6431	0,649224
827	15,0722	13,1966	0,715296
929	19,5872	17,5986	0,920241
1049	34,2923	30,0397	1,7509

Посилаючись на наші попередні результати [2] щодо досліджування метода AGM та метода Сато, можна стверджувати, що метод MSST приблизно у 5 разів є ефективнішим за метод AGM та у 14 разів ефективнішим від найкращої модифікації метода Сато.

На рисунку показано графік залежності розміру поля та часу виконання для різних методів канонічного підйому. Різниця у часі виконання між алгоритмами підйому спостерігається для всіх досліджуваних розмірів розширення поля.

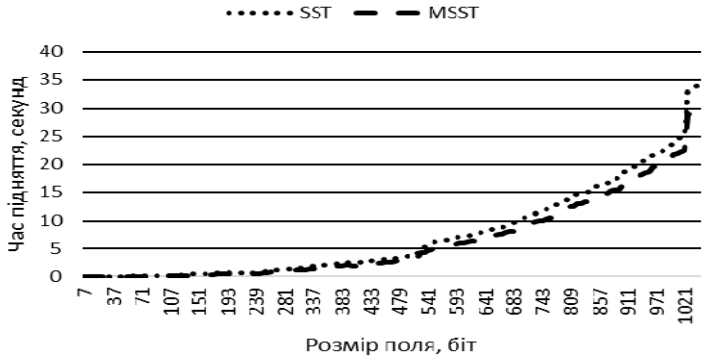

Рисунок. *Графік залежності часу обчислення канонічного підйому від розмірів розширення поля для різних алгоритмів*

Загальний час обчислення кількості точок на еліптичній кривій з розміром 1031 біт, саме такий розмір еліптичних кривих необхідний для надвисокого рівня стійкості (512 біт для симетричного шифру), для метода Харлі з обчисленням норми за SST складає приблизно 10 с, бо виконуються певні операції, які у даній роботі детально не розглядалися зокрема процес генерування поліномів для поля, конвертування елементів перед нормуванням тощо.

Висновки. В даній роботі були проаналізовані алгоритми, що виконують одну з найскладніших та найазартніших з точки зору кількості обчислень задачу під час генерування загальносистемних параметрів, а саме — підняття ізогінеї еліптичної кривої до необхідної точності з метою пошуку сліду ендоморфізму Фробеніуса і відповідно порядку кривої. Нами були проаналізовані алгоритми канонічного підйому еліптичної кривої SST та MSST.

В роботі представлено модифікований алгоритм SST, що може використовуватись для генерування загальносистемних параметрів асиметричних криптоперетворень на базі еліптичних кривих високого та надвисокого рівня стійкості. Теоретична обчислювальна складність даного метода відповідає отриманим експериментальним показникам.

Програмна модель дозволяє згенерувати загальносистемні параметри надвисокого рівня стійкості за секунди.

Список використаних джерел:

1. Gaudry P. A comparison and a combination of SST and AGM algorithms for counting points of elliptic curves in characteristic 2. *ASIACRYPT 2002. 8th International Conference on the Theory and Application of Cryptology and Information Security Queenstown.* New Zealand: Springer, 2002. P. 311–327.
2. Ганзя Р.С. Оцінка обчислювальної складності методів підрахунку кількості точок на еліптичній кривій. Харків: Системи обробки інформації. 2016. Вип. 8(145). С. 92–99.
3. Satoh T., Skjernaa B., Taguchi Y. Fast computation of canonical lifts of elliptic curves and its application to point counting [Text]. *Finite Fields.* 2003. Appl., 9(1). P. 89–101.
4. Frederik Vercauteren. Computing zeta functions of curves over finite fields: dissertation for the degree of PhD: 10.2003. Katholieke Universiteit Leuven, 2013. 195 p.

There was presented modified algorithm for counting order of elliptic curves defined over a binary field. We compared theoretical and experimental performance of computational complexity of this method and its basic version. And we also make conclusions of the possibility of using for modifying national standards.

Key words: *order of elliptic curve, SST method, MSST method.*

Одержано 16.02.2017