Захист інформації

УДК 004.056

Р.С. Ганзя

АТ "Інститут інформаційних технологій", Харків

ОЦІНКА ОБЧИСЛЮВАЛЬНОЇ СКЛАДНОСТІ МЕТОДІВ ПІДРАХУНКУ КІЛЬКОСТІ ТОЧОК НА ЕЛІПТИЧНІЙ КРИВІЙ

В статті наведена коротка характеристика національного та міжнародних стандартів електронних цифрових підписів, описані передумови для генерації загальносистемних параметрів еліптичних кривих високого та надвисокого рівнів стійкості. Проведено теоретичний аналіз існуючих алгоритмів обчислення кількості точок на еліптичних кривих, що визначені над бінарним полем. Реалізовано на практиці алгоритми, що аналізувалися, а за отриманими результатами здійснено порівняння за критерієм складність-стійкість з іншими роботами у даному напрямку. Показані перспективні алгоритми для обчислення порядку еліптичних кривих з подальшою можливістю використання у якості базових параметрів для національного стандарту електронного цифрового підпису.

Ключові слова: *порядок еліптичної кривої, алгоритм Cato, арифметико-геометричний метод, електронний цифровий підпис.*

Вступ

В Україні та у світі, як правило для встановлення конфіденційного ключа симетричного криптоперетворення використовуються асиметричні криптографічні перетворень, які дозволяють вирішити проблему управління ключами, а також розв’язати задачі ідентифікації та автентифікації. Також великою сферою застосування асиметричних критоперетворень є електронний цифровий підпис. На даний момент широко застосовуються асиметричні криптоперетворення побудовані на базі таких математичних апаратів, як поля, кільця та перетворення в групі точок еліптичних кривих. Детальний аналіз математичних апаратів, що застосовуються для криптографічного перетворення інформації можна знайти у [1].

В Україні на рівні національного стандарту (ДСТУ 4145-2002) [2] прийнято алгоритм електронного цифрового підпису, що використовує математичний апарат еліптичних кривих для криптографічного перетворення інформації. Усі асиметричні криптосистеми, що на даний момент застосовуються на міжнародному та національному рівнях в інформаційних система відносяться до класу ймовірностійких. Стійкість таких криптосистем базується на складності вирішення певних математичних проблем (складності факторизації, рішення дискретного логарифму та інших) [1].

Враховуючий швидкий розвиток квантових технологій та існування квантового алгоритму Шора [3], що здатен вирішити наведені вище проблеми факторизації та розв'язання дискретного логарифмічного рівняння із поліноміальною складністю (класичні алгоритми вирішують такі проблеми з субекспоненційної або експоненційної складністю), виникає ситуація, коли сучасні асиметричні криптосистеми можуть бути скомпрометовані [4].

Одним із шляхів вирішення даної проблеми є збільшення розмірів загальносистемних параметрів криптоперетворень. Звичайно таке збільшення не дасть суттєвого підвищення стійкості проти квантового криптоаналізу, проте для проведення такого аналізу необхідний квантовий комп'ютер з великою кількістю кубітів, а як показує аналіз [4, 5] перспектива появи такого комп'ютера в найближчі 5-10 років неможлива. Також перспективним напрямком протидії є дослідження постквантових криптосистем [6].

Враховуючи те, що в Україні були прийняті нові національні стандарти симетричного шифрування (ДСТУ 7624-2014) [7] та геш-функції (ДСТУ 7664-2014) [8] з розмірами блоку повідомлення (виходу геш-функції) та ключа до 512 бітів, то для досягнення однакового рівня стійкості (рівня безпеки) при використанні системи типу "електронний конверт" необхідно використати асиметричне криптоперетворення (електронного цифрового підпису та направленого шифрування) з розмірами загальних параметрів не менше 1024 бітів (надвисокий рівень стійкості).

Національний стандарт електронного цифрового підпису ДСТУ 4145-2002 має загальносистемні параметри з розмірами до 431 біта в стандарті FIPS 186-3 наведено загальносистемні параметри до 521 біта, в міжнародному стандарті ISO\IEC 15946-5 [9], який визначає методи генерації еліптичних кривих також наведено загальносистемні параметри із розміром основного поля до 521 біта. Тому задача ге-

нерування загальносистемних параметрів для еліптичних кривих великих розмірів (1024 біта та більше) є актуальною задачею. В цілому задача генерування загальносистемних параметрів для криптосистем на базі еліптичних кривих зводиться до складного, з точки зору обчислень, завдання – обчислення кількості точок на еліптичній кривій.

Метою цієї статті є визначення основних етапів побудови загальносистемних параметрів еліптичних кривих, аналіз сучасних алгоритмів обчислення порядку еліптичної кривої (підрахунок кількості точок), порівняння за критерієм складність-стійкість алгоритмі обчислення кількості точок на еліптичній кривій з іншими роботами у даному напрямку, Показати перспективні алгоритми для обчислення порядку еліптичних кривих з подальшою можливістю використання у якості базових параметрів для національного стандарту електронного цифрового підпису.

Аналіз сучасних алгоритмів обчислення порядку еліптичної кривої

Нехай E еліптична крива задана рівнянням $y^2 + xy = x^3 + a_6$ з елементом a_6 над F_q з *j-інваріантом* $j(E) = a_6^{-1}$ та $q = p^n$. Кількість точок $\#E(F_q)$ задовольняє співвідношення $\#E(F_q) = q + 1 - t$, де t - слід ендоморфізму Фробеніуса $F : E \to E : (x, y) \to (x^q, y^q)$. За теоремою Хасе [11] отримаємо $|t| \le 2\sqrt{q}$, тому достатньо обчислити $t \bmod B$, де $B > 4\sqrt{q}$.

Схуф описав перший поліноміальний алгоритм для обчислення $\#E(F_q)$, використовуючи *l*-адичний підхід. Часова складність алгоритму Схуфа $O((\log q)^{3\mu+2})$ та просторова складність $O((\log q)^3)$. В подальшому цей алгоритм став основою алгоритма SEA, що має обчислювальну складність $O((\log q)^{2\mu+2})$ та просторову складність $O((\log q)^2)$. Детальний опис можна знайти у [10].

У 1999 році Т. Сато запропонував інший підхід обчислення кількості точок на еліптичній кривій, що базувався на p-адичних числах. Основна ідея даного методу полягала в піднятті кривої та ендоморфізму Фробеніуса до p-адичного кільця та відновлення значення сліду Фроебніуса $t \bmod p^N$ (де $p^N > 4\sqrt{q}$) з даних, які отримані після підняття. Підняття виконується послідовним підняттям j-інваріантів, коефіцієнтів кривої разом з підняттям підгруп l-крутіння з попереднім обчисленням циклу кривих та j-інваріантів j_1 [11].

Канонічний підйом ε звичайної еліптичної кривої E над полем F_q є еліптична крива над Q_q, що задовольняє таким вимогам:

- якщо взяти канонічний підйом ε за модулем p, то це має дорівнювати E із збереженням усіх необхідних властивостей для застосування в криптографічних перетвореннях;
- кільце гомоморфізму $\mathrm{End}(\varepsilon) \to \mathrm{End}(E)$, визваний редукцією за модулем p є ізоморфізмом.

Деурінг показав, що канонічний підйом ε завжди існує і він є єдинним з точністю до ізоморфізма. Наведене вище пояснення є одним із багатьох, якими можна охарактеризувати канонічний підйом.

Нехай E / F_q означає звичайну еліптичну криву а ε / Q_q означає її підйом, тоді наступні твердження є еквівалентними:

- ε канонічний підйом кривої E;
- редукція за модулем p визиває ізоморфізм $\mathrm{End}(\varepsilon) \to \mathrm{End}(E)$;
- піднесення до степені q ізогінея Фробеніуса $\varphi_q \to \mathrm{End}(E)$ піднімається до ендоморфізма $\phi_q \to \mathrm{End}(E)$;
- степінь p ізогінея Фробеніуса $\varphi_q : E \to E^\sigma$ піднімається до ізогінея $\phi_q : \varepsilon \to \varepsilon^\Sigma$ з Σ, що є підстановкою Фробеніуса у Q_q [10].

Остання властивість означає, що існує ізогіней ступеня p між канонічний підйомом ε та його спряженим ε^Σ. Відповідно до властивостей модулярних поліномів степені p $\Phi_p(X, Y) \in Z[X, Y]$, це означає, що $\Phi_p(j(\varepsilon), \Sigma(j(\varepsilon))) = 0$ (теорема Любліна Сьерра та Тейта).

Дана теорема говорить про те, що еліптична крива E визначена над полем $GF\left(p^n\right)$ та має j-й інваріант, який задовольняє умові $j(E) \notin GF\left(p^2\right)$. Тоді існує елемент J, що належить кільцю p-адичних цілих Z_{p^n} такий, що задовольняє умові $\Phi_p\left(J, \sigma^{-1}(J)\right) = 0$ та $J \equiv j \bmod p$.

В даній умові J є j-им інваріантом піднятої кривої ε, яка визначена над розширенням поля p-адичних чисел Q_{p^n}. В теоремі Любліна Сьерра та Тейта для значення $p = 2$ відображення $\sigma^{-1}(J)$ є зворотнім відображенням ендоморфізму Фробеніуса, що діє на елементи розширення кільця 2-адичних цілих Z_{2^n} та належить полю Q_{2^n}, $\Phi_2(x, y)$, є модулярним поліномом. Обчислення значення відо-

браження ендоморфізму Фробеніуса $\sigma(J)$ для елементів поля Q_{2^n} не є простим піднесенням до квадрату з урахуванням правил даного піднесення, як це виконано для відображення Фробеніуса в полі $GF(2^n)$.

Для обчислення сліду ендоморфізма Фробеніуса Сато запропонував не піднімати E окремо, а піднімати всі E в одному циклі одночасно, відповідно до діаграми:

$$\begin{array}{ccccccc} \varepsilon_0 & \xrightarrow{\phi_{p,0}} & \varepsilon_1 & \ldots\ldots & \xrightarrow{\phi_{p,d-1}} & & \varepsilon_0 \\ \downarrow\ \psi & & \downarrow\ \psi & \downarrow\ \psi & & \downarrow\psi & \\ E_0 & \xrightarrow{\varphi_{p,0}} & E\ldots & & \xrightarrow{\varphi_{p,d-1}} & & E_0 \end{array}, \qquad (1)$$

де ε_i є канонічним підйомом E, а $\phi_{p,i}$ є відповідним підйомом $\varphi_{p,i}$.

Для виконання канонічного підйому необхідно вирішити систему рівнянь наступного виду:

$$\begin{cases} \Phi_2(x_0, y_1) = 0; \\ \Phi_2(x_1, y_2) = 0; \\ \ldots\ldots\ldots\ldots\ldots \\ \Phi_2(x_{n-1}, y_0) = 0, \end{cases} \qquad (2)$$

де $\Phi_2(x_{i-1}, y_i)$ є модулярним поліномом. Модулярний поліном для поля характеристики 2 має таке представлення:

$$\begin{aligned} \Phi_2(X,Y) &= X^3 + Y^3 - X^2Y^2 + \\ &+2^4\cdot 3\cdot 31\left(X^2Y + XY^2\right) - \\ &-2^4 3^4 5^3\left(X^2 + Y^2\right) + 3^4 5^3\cdot 4027XY + \\ &+2^8 3^7 5^6\cdot(X+Y) - 2^{12}3^9 5^9, \end{aligned} \qquad (3)$$

де X, Y – змінні.

Розв'язком системи (2) є значення y_i, такі що $y_i = J_i$; $J_i, i = 0,1,2,\ldots,n-1$ є j-інваріантом піднятої кривої ε_i, де $i = 0,1,2,\ldots,n-1$. Розв'язувати дану систему необхідно з використанням метода ітерацій Ньютона для елементів поля Q_{2^n}.

Визначимо відображення $\Theta: Z_q^d \to Z_q^d$ таким чином:

$$\begin{aligned} \Theta(x_0, x_1, \ldots, x_{в-1}) = (&\Phi_2(x_0, x_1), \\ &\Phi_2(x_1, x_2), \ldots, \Phi_2(x_{в-1}, x_0)), \end{aligned} \qquad (4)$$

тоді $\Theta(j(\varepsilon_{d-1}), \Phi_2(\varepsilon_{d-2}), \ldots, \varepsilon_0) = (0,0,\ldots 0)$.

Використовуючи метод ітерацій Ньютона для Θ можна підняти цикл j-інваріантів $\Theta(j(E_{d-1}), \Phi_2(E_{d-2}), \ldots, E_0)$ до Z_q^d з відповідною точністю. Така ітерація задається:

$$\begin{aligned} (x_0, x_1, \ldots, x_{d-1}) \leftarrow &(x_0, x_1, \ldots, x_{d-1}) - \\ &-((D\Theta)^{-1}\Theta)(x_0, x_1, \ldots, x_{d-1}), \end{aligned} \qquad (5)$$

з $(D\Theta)(x_0, x_1, \ldots, x_{d-1})$, що є матрицею Якобіана.

Повна версія алгоритму Сато наведена у роботі [12], основні етапи такого алгоритму це обчислення всіх j-інваріантів та канонічний підйом еліптичної кривої за наведеними вище властивостями. В подальшому метод Сато зазнав певних вдосконалень у напрямку зменшення обчислювальної (хоча і несуттєво) та просторової складності [10].

Інший метод, який дуже сильно пов'язаний з методом Сато базується на арифметико-геометричному методі (AGM) та був запропонований Местре [12] та реалізований Харлі. Харлі також показав, що даний метод може бути надзвичайно ефективним. Обчислювальна складність метода AGM, що був запропонований Местре, не відрізняється від метода Сато, проте має меншу просторову складність. Проте у подальшому AGM був суттєво доопрацьований та модернізований і його складність стала суттєво меншою від складності методу Сато.

Для використання методу AGM необхідна крива E задана рівнянням $y^2 + xy = x^3 + a_6$ з елементом a_6 над F_q з j-інваріантом $j(E) = a_6^{-1}$. Необхідно позначити, що елемент a_6 є довільним елементом з Z_q, що зменшений до a_6 за модулем 2. Далі отримаємо рекурсивну формулу, що дасть нам цілком вірну послідовність (A_i, B_i) елементів з Z_q:

$$\begin{aligned} &A_0 = 1 + 8a_6, \quad B_0 = 1, \\ &A_{i+1} = \frac{A_i + B_i}{2}, \\ &B_{i+1} = \sqrt{A_i + B_i}, \end{aligned} \qquad (6)$$

де квадратний корінь вибирається так, що бути конгруентним до 1 по модулю 4. Таким чином у роботі [13] показано, що якщо квадратний корінь один раз був заданий конгруентним до 1 по модулю 4, то ця пропорція буде зберігатися на кроці $i+1$.

Послідовність (A_i, B_i) називається AGM-послідовністю і її можна привести до послідовності еліптичної кривої E, виразом

$$y^2 = x(x - A_i^2)(x - B_i^2).$$

Позначимо як j_1 j-інваріант еліптичної кривої E.

Добре відомо, що AGM пов'язаний з ізогінезисом степені 2 між еліптичними кривими. Цей крок дає на зв'язок з канонічним підйомом у наступній теоремі.

Нехай j_1 буде j-інваріантом еліптичної кривої E пов'язаний з AGM послідовністю. Тоді послідовність j_i підтверджує:

$$\begin{aligned} &j_0 \equiv a_6^{-2} \bmod 2, \\ &j_{i+1} \equiv j_i^2 \bmod 2, \\ &j_i \equiv j_i^{\uparrow} \bmod 2^{i+2}. \end{aligned} \qquad (7)$$

Перше твердження показує, що E ізоморфна зі сполученим підйомом з початковою еліптичною кривою E по модулю 2. Друге – стверджує, що всі еліптичні криві E_i також зменшуються за модулем 2 до сполучень кривої E (з точністю до ізоморфізму). Третє є основною AGM алгоритму: це означає, що, коли відбувається підйом по AGM-послідовності, ми все ближче і ближче наближаємось до канонічного підйому.

Це дає простий алгоритм для обчислення канонічного підйому. Починаючи з початкових значень (A_0, B_0), ми застосовуємо рекурсивну формулу для обчислення послідовних значень (A_i, B_i). Після k кроків, ми можемо обчислити j-інваріант асоційованої кривої, близький до канонічного підйому сполученої E піднятої до точності 2^k [13].

Зв'язок цієї теореми зі слідом Фробеніуса дає нам ефективний метод для підрахунку кількості точок еліптичної кривої E.

Нехай $i > 0$ та нехай c_i буде

$$\mathrm{Norm}_{Z_q/Z_p}\left(A_{i+1}/A_i\right)$$

тоді:

$$c_i + q/c_i = \mathrm{Tr}(E) \bmod 2^{i+4}. \qquad (8)$$

AGM алгоритм складається з таких частин: спочатку обчислюється AGM-послідовність з достатньою кількістю кроків, а далі йде обчислення норми, що дає слід початкової кривої з деякою точністю, яка дорівнює числу кроків плюс константа. На перший погляд, здається, що ми повинні починати з великої точності для A_0 та B_0, тому що ми отримуємо все менше і менше значущі цифри у A_i та B_i, коли в той же час j_i стає ближче до канонічного підйому. Ця проблема може бути вирішена шляхом додавання довільного шуму до A_i та B_i перед операцією, яка "понижує" точність, як квадратний корінь або ділення на 2.

Нижче наведено кроки виконання арифметико-геометричного методу для підрахунку кількості точок на еліптичній кривій $E(F_{2^d})$, що був запропонований Местре [12].

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

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

1. $N \leftarrow \lceil d/2 \rceil + 3$.
2. $a \leftarrow 1$ and $b \leftarrow (1 + 8c) \bmod 2^4$.
3. for $i = 5$ to N do
4. $(a, b) \leftarrow ((a+b)/2, \sqrt{ab}) \bmod 2^i$.
5. $a_0 \leftarrow a$.
6. for $i = 0$ to $d - 1$ do
7. $(a, b) \leftarrow ((a+b)/2, \sqrt{ab}) \bmod 2^N$.
8. $t \leftarrow a_0 / a \bmod 2^{N-1}$.
9. if $t^2 > 2^{d+2}$ then $t \leftarrow t - 2^{N-1}$.
10. return $2^d + 1 - t$.

Другий цикл обчислень, що починається на 6 кроці, можна замінити на обчислення однієї арифметико-геометричної ітерації та обчислення норми. Тобто

$$t \equiv N_{Q_p/Q_p}(a_0 / a_1) \pmod{2^N}. \qquad (9)$$

Таке саме вдосконалення можна зробити і для алгоритму Сато, спираючись на пояснення в роботі [10] і замінити цикли обчислень сліду ендоморфізму Фробеніуса на обчислення однієї ітерації та нормування коефіцієнту c_0^2, попередньо обчисливши його квадратний корінь, таким чином отримаємо таке:

$$t \equiv N_{Q_p/Q_p}(c_0) \pmod{2^N}. \qquad (10)$$

Для обчислення норми можна використати декілька алгоритмів: аналітичний (запропонований Сато, Ск'єрною та Тагучі), а також метод на основі результанта. Для обчислення результанта було запропоновано використати швидкий алгоритм обчислення найбільшого спільного дільника, який показав Моенк [14].

У [13] Гаудрі запропонував замінити AGM-послідовність (A_i, B_i), що є двозмінною (AGM bivariate) на однозмінну (AGM univariate). Тобто можна взяти одну зміну і визначити її наступним чином:

$$\lambda_i = A_i / B_i. \qquad (11)$$

Відповідні еліптичні криві мають вираз $y^2 = x(x-1)(x-\lambda_i^2)$. Таким чином з виразу 5 можна показати виходить що λ_{i+1} обчислюється таким чином:

$$\lambda_{i+1} = \frac{1+\lambda_i}{2\sqrt{\lambda_i}}. \qquad (12)$$

Таким чином однозмінний AGM алгоритм обчислення кількості точок на еліптичній кривій з заміною другого циклу обчислень на обчислення норми має такі кроки:

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

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

1. $N \leftarrow \lceil d/2 \rceil + 3$.
2. $\lambda \leftarrow (1 + 8c) \bmod 2^4$.
3. for $i = 5$ to N do
4. $\lambda \leftarrow \left((1+\lambda)/\left(2\sqrt{\lambda}\right)\right) \bmod 2^i$.
5. $t = \mathrm{Norm}\left(2\lambda/(1+\lambda)\right) \bmod 2^{N-1}$.
6. if $t^2 > 2^{d+2}$ then $t \leftarrow t - 2^{N-1}$.
7. return $2^d + 1 - t$.

Запропонована модифікація AGM методу, тобто перехід від двох змінних до однієї не повинна зменшити обчислювальну складність частини підйому, проте в даному випадку є незначний виграш у просторовій складності. Дана модифікація була запропонована Гаудрі для переходу до модифікованого методу SST (MSST), що являє собою модифікацію методу AGM та SST, опис даного методу можна знайти у [13]. Дослідження методу SST та MSST є наступним кроком наших досліджень, пов'язаних з ефективними методами формування загальносистемних параметрів для криптосистем на еліптичних кривих, в тому числі для національного стандарту ДСТУ 4145-2002. У методі SST (Сато, Ск'єрна і Тагучі) [15] було запропонованоновий метод знаходження кількості точок на еліптичній кривій, змінивши представлення Z_q. Проте запропонований алгоритм, вимагає етапу передобчислень, але це зовсім не проблема для великих криптографічних розмірів, де це легко здійснити і зберігати з попередньо обчислюваними даними.

Оптимальним на сьогодні методом обчислення кількості точок на еліптичній кривій як показує теоретичний аналіз є метод, запропонований Харлі [16], в якому запропоновано інший метод вирішення модулярного полінома $\Phi_p(X, Y)$.

Множення двох цілих чисел, що складаються з n біт, здійснено за $O\left(n^{\mu}\right)$ операцій, де μ – це константа, яка визначає час виконання множення двох m бітових цілих чисел з часовою складністю $O\left(m^{\mu}\right)$. Так для класичних алгоритмів множення значення $\mu = 2$ для швидкого алгоритму Карацуби, слідуючи роботі [10], $\mu = \log_2 3$.

Слід зазначити, що кожний з наведених методів знаходить лише порядок кривої та не відповідає на запитання можливості її використання в криптографічних перетвореннях. Виходячи з цього, після обчислення порядку кривої необхідно з'ясувати придатність її до застосування в криптографічних системах. Вибрати критерії, які дозволяють обирати еліптичні криві для побудови загальносистемних параметрів необхідного рівня стійкості.

Практичні результати у побудові сильних криптографічних параметрів еліптичних кривих

При дослідженні механізмів побудови сильних криптографічних загальносистемних параметрів еліптичних кривих для їх подальшого застосування у механізмах електронного цифрового підпису за ДСТУ 4145-2002 (або аналогічних, тобто тих, що використовують бінарне поле), важливим критерієм є час, що необхідний для побудови таких параметрів та вимірність поля над яким визначена крива. Так як в національному стандарті визначені параметри з розмірами до 431 біта, а в стандарті FIPS 186-3 наведено загальносистемні параметри до 521 біта, то важливим є оцінка часу для побудови сильних криптографічних параметрів надвисокого рівня стійкості ($509 \le \#E \le 1031$, біт) [1].

Найбільшу складність та затратність ресурсів при генерації параметрів займає крок обчислення кількості точок на еліптичній кривій. При дослідженні цього кроку було використано два різні методи для канонічного підйому еліптичної кривої та два різні методи для циклу нормування коефіцієнтів з метою отримання значення сліду ендоморфізму Фробеніуса.

Для канонічного підйому було використано арифметико-геометричного метод (AGM) [13] та методі Сато[11] (описані у п.4). Для обчислення норми було використано, окрім додаткових циклів AGM та методу Сато, аналітичний метод (запропонований Сато, Ск'єрною та Тагучі, SST нормування) [15], а також метод на основі результата [14].

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 табл. 1 наведено час обчислення фази підйому та норми для різних варіантів AGM методу (двозмінного та однозмінного), а наведено час обчислення фази підйому та норми для найбільш оптимального методу Сато (модифікації Веркаутерена [10]). За результатами аналізу табл. 1 можна стверджувати, що різниця для фази підйому для двозмінного та однозмінного алгоритму AGM не спостерігається, проте різниця для різних алгоритмів обчислення норми спостерігається. Найбільш ефективним є метод нормування SST.

На рис. 1 показано графік залежності розміру поля та часу підйому для різних методів канонічного підйому. Так як двозмінний та однозмінний методи AGM мають невелику різницю у часі роботи, то їх суттєва різниці на графіку не відображається, проте різниця у часі виконання для методу Сато (модифікація Веркаутерена) та для AGM спостерігається для всіх досліджуваних розмірів розширення поля.

Можна стверджувати, що канонічний підйому еліптичної кривої з використанням арифметико-геометричного методу приблизно у три рази ефективніший від методу Сато (навіть його найкращої модифікації).

Таблиця 1

Обчислювальна складність p-адичних методів

Степінь розширення поля d, біт	Фаза підйому			Обчислення норми			
	AGM bivariate (двозмінний), с	AGM univariate (однозмінний), с	Метод Сато (модифікація Веркаутерена), с	Додатковий цикл за Местре, с	Додатковий цикл (модифікація Веркаутерена), с	Обчислення результанта, с	Нормування за SST
7	0,001038	0,000938	0,018552	0,002122	0,017289	0,0009	0,000236
23	0,015002	0,01483	0,085095	0,041987	0,143847	0,002081	0,000947
79	0,247437	0,255037	1,45561	0,65108	3,53269	0,033835	0,009164
107	0,527144	0,507134	2,66313	1,29144	2,66313	0,078065	0,016757
173	1,88726	1,92282	9,26296	5,17245	9,26296	0,349419	0,051377
199	2,58677	2,59791	12,458	6,62534	35,5715	0,508944	0,080368
257	2,59583	2,59573	10,6567	8,03255	38,6613	1,24161	0,185441
307	4,55193	4,57529	17,5725	13,7089	63,0424	2,09486	0,241653
383	7,19335	7,2112	26,8963	21,6217	94,4539	4,45025	0,527865
433	9,29693	9,30088	34,2528	27,6736	119,773	6,2283	0,810655
503	12,7932	12,7955	46,55	37,9071	181,273	10,1295	1,23282
601	26,8153	26,6644	91,6184	86,1802	363,051	19,2975	2,8489
709	37,9417	37,5102	127,882	123,696	496,369	35,9172	4,15462
787	47,648	47,8452	158,045	152,693	615,89	55,7415	7,56451
827	52,9663	53,0276	175,664	171,616	679,553	68,2506	7,92211
929	67,0609	67,0016	221,279	218,492	856,731	103,512	11,4582
1021	82,083	81,5745	285,803	281,817	1213,3	156,275	20,2189
1049	131,367	131,111	429,016	458,253	1892,64	169,589	26,076

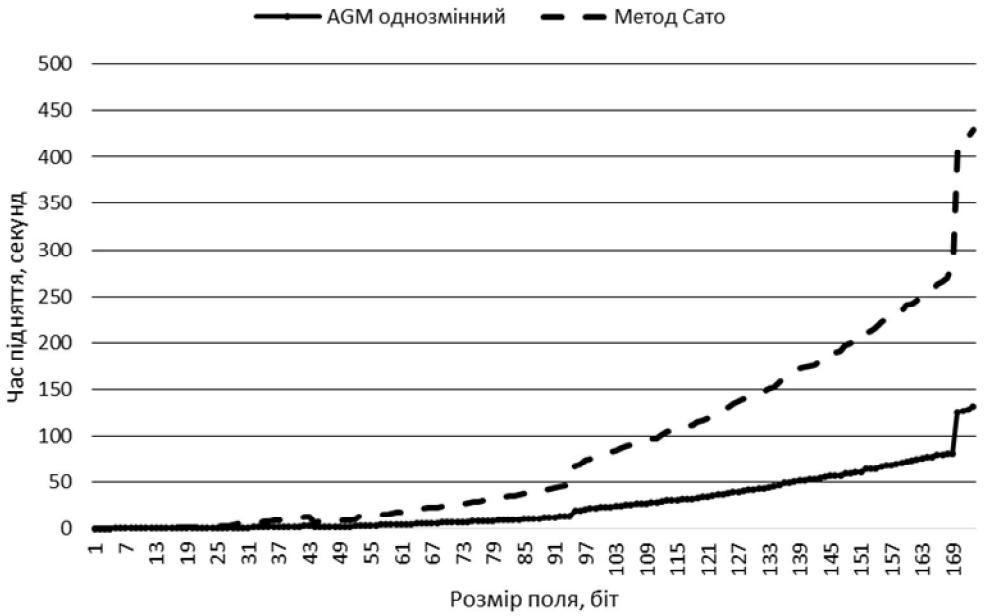

Рис. 1. Графік залежнсті часу обчислення канонічного підйому від розмірів розширення поля для різних алгоритмів

На рис. 2 показано графік залежності розміру поля та часу обчислення норми для різних методів. На графіку видно, що використання додаткових циклів, як AGM, так методу Сато, не є ефективним. Найбільш ефективним є метод обчислення норми SST. Метод на основі результанта вимагає більшої кількості обчислювальних ресурсів, проте його можна розпаралелити за рахунок того, що обчислення виконуються в масиві (матриці).

Можна стверджувати, що нормування коефіцієнтів для отримання значення сліду ендоморфізму Фробеніуса необхідно виконувати за методом SST, щоб досягти найменшої обчислювальної складності.

Отримані результати можна порівняти з результатами, що міться у роботі Веркаутерена [10]. Для обчислення кількості точок на еліптичній кривій він використав процесор AMD XP 1700+ та операційну систему Linux Redhat7.1. Алгоритми написанні на мові програмування C, а базові математичні операції в кільці p-адичних чисел виконані на Асемблері.

Результат порівняння часових показників Веркаутерана та отриманих нами показано в табл. 2 (стовпчики з даними Веркаутерена містять позначку "B").

Рис. 2. Графік залежнсті часу обчислення норми від розмірів розширення поля для різних лгоритмів

Таблиця 2

Порівняння часової складності обчислення порядку кривої з іншими роботами

Розширення поля d, біт	Загальний час обчислення порядку кривої				
	Метод Сато (модифікація Веркаутерена)	Метод Сато (модифікація Веркаутерена) "B"	AGM	AGM "B"	Метод Харлі [16] "B"
144	22,3	1,91	4,2	0,57	0,06
168	33,6	3,22	6,5	0,88	0,08
192	43,4	4,62	8,3	1,39	0,12
240	38,2	10,9	7,7	2,81	0,25
288	70,9	17,6	15,8	5,44	0,38
336	97,6	30,2	22,3	9,28	0,6
384	121,3	49,3	28,8	15,4	0,92
480	188,5	106,5	45,7	34,5	1,87

Результати з табл. 2 показують, що базові математичні операції написані на низькорівневій мові програмування (реалізовані Веркатуереном) дають велику ефективність при обчислені порядку еліптичної кривої. Найефективнішим методом для обчислення порядку еліптичної кривої, як показано в табл. 1 і на практиці в табл. 2 Веркаутереном, є метод Харлі.

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 однозмінного AGM алгоритму з обчисленням норми за SST складає приблизно 132 с. Для того, щоб досягнути криптографічної стійкості загальносистемних параметрів визначено певний ряд умов, і якщо значення порядку кривої (кількості точок) не задовольняє хоча б однієї з цих умов, то таке значення не можливе для використання у криптосистемах для досягнення зазначеного рівня стійкості.

Висновки

1. Таким чином на даний момент існують загрози для асиметричної криптографії. Такі загрози пов'язані з квантовим алгоритмом Шора. Для підвищення стійкості сучасних асиметричних алгоритмів можна збільшити розмір базової точки. Звичайно таке збільшення не дасть суттєвого підвищення стійкості проти квантового криптоаналізу, проте для проведення такого аналізу необхідний квантовий комп'ютер з великою кількістю кубітів

2. Сучасні тенденції у напрямку розвитку національної криптографії (нові національні стандарти симетричного шифрування ДСТУ 7624-2014 та геш-функції ДСТУ 7664-2014) з розмірами блоку повідомлення (виходу геш-функції) та ключа до 512 бітів вимагають використання асиметричної криптографії з таким самим (надвисоким) рівнем стійкості (для еліптичних кривих 1021-1031 біт).

3. Найбільш ефективним методом для обчислення порядку еліптичної кривої (як показує теоретичний аналіз) є метод Харлі. Даний алгоритм є еволюцією метода Сато та арифметико-геометричного методу, що використовує інший базис та власний алгоритм для обчислення норми.

4. Було розроблено програмну модель AGM методу та методу Сато. Проведено аналіз обчислювальної складності оригінального AGM методу (запропонованого Местре) та однієї з його модифікації (запропонованої Гаудрі), а також декілька варіантів обчислення норми. Для побудови ефективних алгоритмів генерування загальносистемних параметрів для еліптичних кривих процес вибору алгоритмів нормування є важливим. Якщо крок підняття еліптичних кривих неможливо розпаралелити при його обчисленні, тому що даний крок є рекурсивним, то крок нормування можна розпаралелити, при виборі

відповідного алгоритму нормування. Проте як показує аналіз вибір методу SST для нормування є оптимальним.

5. Практичні результати отримані нами в декілька разів гірші від результатів, що отримані Веркаутереном. Це пояснюється тим, що він використав у програмах власну бібліотеку (написано на Асемблері) для виконання базових математичних операцій при обчислені порядку кривої.

Список літератури

1. Горбенко І.Д. Прикладна криптологія [Текст]: монографія / І.Д. Горбенко, Ю.І. Горбенко. – Х.: Форт, 2012. – 868 с.

2. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що грунтується на еліптичних кривих. Формування та перевірка. ДСТУ 4145-2002 – [Чинний від 2003-07-01]. – К.: Держстандарт України, 2003. – 31 с.

3. Shor P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer [Text] / P.W. Shor //SIAM J. Comput. – 1997. – 26 (5). – P. 1484-1509.

4. Ганзя Р.С. Аналіз можливостей квантових комп'ютерів та квантових обчислень для криптоаналізу сучасних криптосистем / Р.С. Ганзя, Ю.І. Горбенко // Восточно-Европейский журнал передовых технологий. – 2014. – Т. 6, № 1 (67). – С. 8-15.

5. Горбенко Ю.І. Аналіз шляхів розвитку криптографії після появи квантових комп'ютерів / Р.С. Ганзя, Ю.І. Горбенко // Вісник Національного університету "Львівська політехніка": "Комп'ютерні системи та мережі". – 2014. – № 806. – С. 40-48.

6. A riddle wrapped in an enigma [Electronic resource] / IACR General Secretariat, Santa Rosa Administrative Center, University of California, Santa Barbara, CA 93106-6120, USA, N. Koblitz. A. Menezes. – Режим доступа : www/ URL: — https://eprint.iacr.org/2015/1018.pdf . – 03.02.2016.

7. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. ДСТУ 7624:2014.

8. Інформаційні технології. Криптографічний захист інформації. Функція гешування. ДСТУ 7664:2014.

9. ISO/IEC 15946-5:2009. Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 5: Elliptic curve generation. 2014-04-10 – CH-1211 Geneva 20, – 2009 – 31 p.

10. Frederik Vercauteren. Computing zeta functions of curves over finite fields: dissertation for the degree of PhD: 10.2003 Frederik Vercauteren. – Katholieke Universiteit Leuven, 2013. – 195 p. – Bibliogr. : pp. 171–181.

11. Satoh T. Canonical lifting of elliptic curves and p-adic point counting. (theoretical background) / T. Satoh // Department of Mathematics, Faculty of Science, Saitame University. – 2001. – P. 1–21.

12. Mestre, J.F. AGM pour le genre 1 et 2. [Text] / J.F. Mestre // Lettre à Gaudry et Harley - December 2000. 9. Miller V. Uses of elliptic curves in cryptography Advances in Cryptology Proceedings of Crypto Lecture Notes in Computer Science / Miller V. Springer – Verlag New-York, 1986. – P. 417–426.

13. Gaudry, P. A comparison and a combination of SST and AGM algorithms for counting points of elliptic curves in characteristic 2 / P. Gaudry // ASIACRYPT 2002. 8th International Conference on the Theory and Application of Cryptology and Information Security Queenstown - New Zealand: Springer, 2002 – P.311-327.

14. Cohen, H. Elliptic and Hyperelliptic Curve Cryptography [Text]: handbook / H. Cohen, G. Frey – NW.: Chapman & Hall/CRC, 2006. - 807 p.

15. Satoh, T. Fast computation of canonical lifts of elliptic curves and its application to point counting [Text] / T. Satoh, B. Skjernaa, Y. Taguchi // FiniteFields. – 2003. – Appl.,9(1). – pp. 89-101.

16. Harley, R. Asymptotically optimal p-adic point-counting [Text]/ E-mail to NMBRTHRY list – December, 2002.

Надійшла до редколегії 12.05.2016

Рецензент: д-р техн. наук, проф. І.Д. Горбенко, Харківський національний університет ім. В.Н. Каразіна, Харків.

ОЦЕНКА ВЫЧИСЛИТЕЛЬНОЙ СЛОЖНОСТИ МЕТОДОВ ПОДСЧЕТА КОЛИЧЕСТВА ТОЧЕК НА ЭЛЛИПТИЧЕСКОЙ КРИВОЙ

Р.С. Ганзя

В статье приведена краткая характеристика национального и международных стандартов электронных цифровых подписей, описаны предпосылки для генерации общесистемных параметров эллиптических кривых высокого и сверхвысокого уровней устойчивости. Проведен теоретический анализ существующих алгоритмов вычисления количества точек на эллиптических кривых, определенных над бинарным полем. Реализовано на практике алгоритмы, которые анализировались, а по полученным результатам проведено сравнение по критерию сложность-стойкость с другими работами в данном направлении. Показаны перспективные алгоритмы для вычисления порядка эллиптических кривых с последующей возможностью использования в качестве базовых параметров для национального стандарта электронной цифровой подписи.

Ключевые слова: *порядок эллиптической кривой, алгоритм Camo, арифметико-геометрический метод, электронная цифровая подпись.*

EVALUATION OF THE COMPUTATIONAL COMPLEXITY OF ELLIPTIC CURVES POINT COUNTING METHODS

R.S. Hanzia

The article provides a short description of national and international standards for digital signatures and describes conditions for the generation general system parameters of elliptic curves of high and ultra-high levels of security. We show theoretical analysis of existing algorithms for calculating the number of points on elliptic curves defined over the binary field. Implementing in practice algorithms that were analyzed, and the obtained results were compared by the criterion of difficulty-resistance with other works in this direction. Showing perspective algorithms to calculate the order of elliptic curves with the possibility of using as basic parameters for a national standard of digital signature.

Keywords: *order of the elliptic curve, Satoh's algorithm, arithmetic-geometry mean, electronic digital signature.*