УДК 621.391.7

МЕТОД ЦИФРОВОГО ПІДПИСУВАННЯ НА ОСНОВІ МАТЕМАТИЧНОГО АПАРАТУ ЕЛІПТИЧНИХ КРИВИХ З ПРИСКОРЕНОЮ ПРОЦЕДУРОЮ ПЕРЕВІРКИ ПІДПИСУ

Юрій Яремчук, Костянтин Черняхович
Вінницький національний технічний університет

Анотація: **Запропоновано метод цифрового підписування на основі математичного апарату еліптичних кривих для застосування в додатках, що потребують швидкої перевірки цифрового підпису.**
Summary: **This work proposes the method of the digital signature based on the mathematical background of elliptic curves for being used in applications that requires a high-speed verification of digital signature.**
Ключові слова: **Захист інформації, криптографія, цифровий підпис, еліптичні криві.**

I Вступ

Системи криптографічного захисту інформації на сьогодні набули широкого застосування в галузі інформаційних технологій. Особливу роль серед криптографічних методів захисту займають методи цифрового підписування (ЦП), які надають можливість вирішувати такі важливі задачі криптографічного захисту як цілісність, автентичність та неможливість відмови від авторства.

Серед існуючих методів ЦП найбільш поширеними є RSA, DSA [1] та методи на основі математичного апарату еліптичних кривих (ЕК) ECDSA та ECSS [2 – 4].

На сьогодні методи ЦП використовуються для вирішення конкретних прикладних задач, зокрема таких як:

забезпечення безпеки банківських трансакцій;
забезпечення безпеки електронного документообігу;
забезпечення безпеки електронних платіжних систем та електронної комерції (e-commerce);
засвідчення авторства при електронному голосуванні (e-voting);
підписування повідомлень електронної пошти;
підписування DNS-зон (DNS-zone signing);
підписування XML документів;
автентифікація в безпровідних мережах (Wi-Fi);
забезпечення безпеки мобільної комерції (m-commerce);
автентифікація та ідентифікація в системах стільникового зв'язку;
підписування цифрових сертифікатів та цифрових паспортів на базі смарт-карток;
автентифікація в кишенькових персональних комп'ютерах та смартфонах.

Однак, при застосуванні відомих методів ЦП для вирішення цих задач виникає проблема, пов'язана з тим, що практично в усіх цих задачах перевірку цифрового підпису необхідно здійснювати значно частіше, ніж його формування, і перевіряти підпис від великої кількості його власників. В цьому випадку сторона, яка перевіряє, за одиницю часу може отримувати велику кількість запитів на перевірку підпису, що, в свою чергу, може призводити до її перевантаження.

II Аналіз швидкості формування-перевірки підпису сучасних методів цифрового підписування. Постановка задачі

З метою дослідження ефективності застосування сучасних методів ЦП щодо вирішення вказаної проблеми проведено аналіз швидкості формування-перевірки підпису відомих методів ЦП.

В табл. 1 наведено результати аналізу методу ECDSA щодо швидкості формування/перевірки підпису для різних довжин ключів.

Таблиця 1 – Співвідношення швидкості формування/перевірки підпису за методом ECDSA

Довжина ключа, біт	Кількість сформованих підписів за секунду	Кількість перевірених підписів за секунду	Співвідношення кількості сформованих підписів до кількості перевірених за секунду
224	1764	792	2.2 : 1
256	900	380	2.4 : 1
384	516	184	2.8 : 1
521	240	88	2.8 : 1

З результатів, які наведено в табл. 1, видно, що формування цифрових підписів за методом ECDSA виконується приблизно в 2,5 рази швидше, ніж його перевірка.

В табл. 2 наведено результати аналізу порівняння часу формування/перевірки одного підпису на прикладі відомих методів RSA та ECDSA. Під час аналізу методів ЦП довжину ключа для методу ECDSA взято розміром 224 біт, а для методу RSA - 2048 біт, що відповідає рівню криптостійкості методу ECDSA з довжиною ключа 224 біти.

Таблиця 2 – Співвідношення часу виконання процедур формування/перевірки одного цифрового підпису відомих методів ЦП

Довжина ключа, біт		Формування RSA / ECDSA	Перевірка RSA / ECDSA
ECDSA	RSA		
191	1024	1:12	30:1
224	2048	1:59	13:1

З наведених в табл. 2 результатів видно, що за методом ECDSA на перевірку цифрового підпису витрачається приблизно в 13 разів більше часу, ніж за методом RSA. При цьому на формування підпису за методом ECDSA потрібно приблизно в 59 разів менше часу, ніж за RSA.

Отже, з отриманих результатів аналізу можна зробити такі висновки. Метод на основі математичного апарату ЕК ECDSA має складну, з точки зору обчислень, процедуру перевірки ЦП і потребує значно більше часу для перевірки цифрового підпису порівняно з методом RSA. Однак, використання самого математичного апарату ЕК для побудови методів ЦП є доцільним та перспективним, тому що ці методи використовують значно менші довжини ключів та загальносистемних параметрів. Тобто, актуальними є дослідження, спрямовані на прискорення перевірки цифрового підпису методів ЦП на основі математичного апарату ЕК.

В цьому зв’язку, слід звернути увагу на роботи [5 – 7], в яких з метою підвищення швидкості процесу перевірки цифрового підпису на прикладі методу ECDSA запропоновано модифікації з прискореною процедурою перевірки цифрового підпису за рахунок використання передобчислень. Однак, отримані результати не забезпечують суттєвого збільшення швидкості перевірки цифрового підпису. Крім того, основним недоліком цих методів є те, що результати передобчислень потрібно постійно зберігати в пам’яті системи цифрового підписування, що створює додаткові труднощі.

Виходячи з вищесказаного сьогодні актуальними є дослідження, спрямовані на підвищення швидкості перевірки цифрового підпису методів ЦП, що базуються на математичному апараті ЕК для використання в задачах, де навантаження на процедури перевірки цифрового підпису є критичним.

III Метод вдосконалення цифрового підписування на основі еліптичних кривих

Аналіз більшості методів ЦП на основі математичного апарату ЕК показав, що в основі процедури перевірки підпису цих методів лежить рівняння вигляду

$$R = aP + bQ, \tag{1}$$

де P – базова точка ЕК порядку n; Q – точка ЕК порядку n, як відкритий ключ; $a < n$, $b < n$ – цілі числа, які обчислюються на основі значень r та s – складових цифрового підпису, який перевіряється.

З виразу (1) видно, найскладнішою в ньому є операція скалярного добутку великого цілого числа на точку ЕК. Причому таких операцій в (1) – дві. При цьому в процедурі формування підпису, на відміну від процедури перевірки підпису, використовується лише одна операція скалярного добутку великого цілого числа на точку ЕК.

Зважаючи на це, одним із можливих шляхів зменшення обчислювальної складності процедури перевірки цифрового підпису може бути спрощення виразу (1) за рахунок збільшення обчислювальної складності процедури формування цифрового підпису, оскільки ця процедура має значно меншу обчислювальну складність ніж процедура перевірки. Це стає можливим завдяки тому, що процедури перевірки та формування цифрового підпису безпосередньо пов’язані між собою.

Виходячи з цього, пропонується метод ЦП на основі математичного апарату ЕК (заявка на корисну модель № u2007 05052 від 07. 05. 2007 р.), основна ідея якого полягає в зведенні до мінімуму найбільш обчислювально складних операцій в процедурі перевірки цифрового підпису за рахунок допустимого збільшення обчислювальної складності в процедурі формування цифрового підпису.

Наприклад, якщо з виразу (1) перенести у процедуру формування підпису одну операцію скалярного множення цілого числа на базову точку ЕК, тобто aP, то можна отримати спрощення виразу (1) до однієї операції скалярного множення великого цілого числа на точку ЕК.

Пропонується, на відміну від відомих методів ЦП на основі математичного апарату ЕК, в процедурі перевірки цифрового підпису замість виразу (1) для перевірки цифрового підпису $\{s, r\}$ використовувати спрощені з точки зору обчислювальної складності вирази вигляду

$$r' = (s - h'm'') \bmod n, \tag{2}$$

$$r'' = (rm'') \bmod n, \tag{3}$$

де n – порядок базової точки ЕК, h' – обчислений геш-код у вигляді цілого числа від повідомлення *M*, m'' – велике ціле число, обчислене за формулою

$$m'' = \vartheta(\lambda(rQ)),$$

де r – велике ціле число – елемент цифрового підпису, $\vartheta(\cdot)$ – функція перетворення елементу скінченого поля у велике ціле число, $\lambda(\cdot)$ – функція перетворення точки ЕК в елемент скінченого поля, Q – точка ЕК як відкритий ключ, обчислений за виразом

$$Q = dP, \tag{4}$$

де d - велике ціле число, як таємний ключ.

Для перевірки підпису пропонується порівнювати обчислене за виразом (2) велике ціле число r' із обчисленим за виразом (3) великим цілим r''. Використання виразів (2) та (3) замість (1) дозволяє зменшити обчислювальну складність процедур перевірки цифрового підпису, що приводить до прискорення перевірки цифрового підпису.

Для забезпечення можливості перевірки цифрового підпису за виразами (2) та (3) формування цифрового підпису пропонується здійснювати на основі виразу

$$s = m'(r + h) \bmod n, \tag{5}$$

де h – велике ціле число, як геш-код від повідомлення M, який обчислюється за допомогою функції гешування H, r – елемент цифрового підпису як велике ціле число, що обчислюється за виразом вигляду

$$r = \vartheta(\pi(h)x_R) \bmod n, \tag{6}$$

де $\pi(\cdot)$ – функція перетворення великого цілого числа на елемент скінченого поля, x_R – елемент скінченого поля, який обчислюється як

$$x_R = \lambda(R), \tag{7}$$

де R – точка ЕК, яка обчислюється за виразом вигляду

$$R = kP, \tag{8}$$

де k – тимчасовий таємний ключ у вигляді великого випадкового цілого числа, P – базова точка ЕК, m' – велике ціле число, яке обчислюється як

$$m' = \vartheta(x_L), \tag{9}$$

де x_L – елемент скінченого поля, який обчислюється за виразом вигляду

$$x_L = \lambda(L), \tag{10}$$

де L – точка ЕК, що обчислюється за виразом вигляду

$$L = zP, \tag{11}$$

де z – велике таємне ціле число, яке обчислюється як

$$z = dr \bmod n. \tag{12}$$

Загальна схема методу ЦП на основі математичного апарату ЕК, що пропонується, буде мати вигляд, представлений на рис. 1.

Згідно з запропонованим методом, спочатку потрібно сформувати загальносистемні параметри. Загальносистемними є такі параметри: m - степінь розширення основного поля; еліптична крива E:

$$y^2 + xy = x^3 + Ax^2 + B, \tag{13}$$

n – ціле число, як порядок базової точки ЕК; P – базова точка ЕК; d – таємний ключ; Q – відкритий ключ; k – тимчасовий таємний параметр, як випадкове велике ціле число; H – обрана функція гешування.

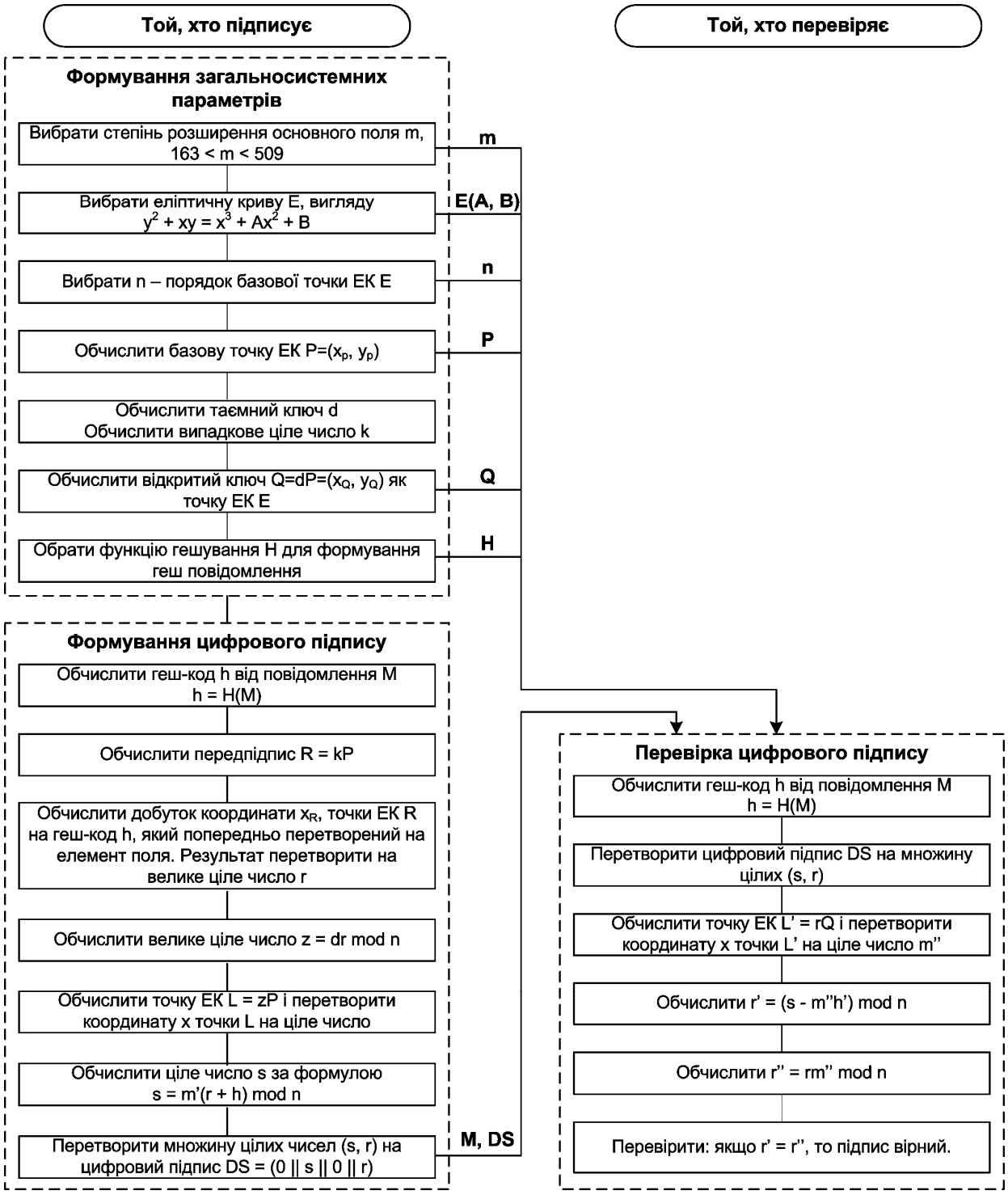

Рисунок 1 – Схема запропонованого методу ЦП на основі математичного апарату ЕК з прискореною перевіркою підпису

Після того, як сформовано загальносистемені параметри, сторона, яка підписує, здійснює формування цифрового підпису для повідомлення M. Для цього необхідно виконати такі дії. Обчислити геш-код h як велике ціле число за допомогою обраної функції гешування H від повідомлення M. Обчислити передпідпис R як точку ЕК. Обчислити велике ціле число r як добуток елементу скінченого поля у вигляді координати x точки R ЕК на попередньо перетворений в елемент скінченого поля геш-код h, а

результат обчислень перетворити на ціле число. Обчислити ціле число z як добуток таємного ключа d на велике ціле число r. Обчислити точку ЕК L як скалярний добуток таємного цілого числа z на базову точку ЕК P. Отриману точку L перетворити на ціле число m'', що використовується для забезпечення можливості відновлення контрольного параметру, який бере участь в обчислені великого цілого числа s. Число s обчислити як суму великих цілих чисел r та h, помножених на велике ціле m''. Отриману множину цілих чисел $\{s, r\}$ перетворити на цифровий підпис вигляду $DS = \{0 \,||\, s \,||\, 0 \,||\, r\}$.

Після цього, одержувач цифрового підпису (той хто перевіряє), використовуючи загальносистемні параметри, повідомлення M та цифровий підпис DS, може перевірити його, виконавши такі дії. Обчислити геш-код h' як ціле число від повідомлення M, використовуючи задану функцію гешування H. Перетворити цифровий підпис DS на множину цілих $\{s, r\}$. Обчислити точку ЕК L' як скалярний добуток цілого числа r на відкритий ключ Q. Результат обчислення L' використати для відновлення точки ЕК вигляду drP, яку було обчислено в процесі формування цифрового підпису. Обчислити елемент основного поля як x'_L на основі точки ЕК L' та перетворити його на велике ціле число m''. Обчислити великі цілі числа r' та r'' відповідно за формулами (2) та (3). Якщо $r' \equiv r''$, то вважати, що цифровий підпис DS вірний.

Таким чином, запропоновано метод цифрового підписування, який має лише одну операцію скалярного добутку цілого числа на точку ЕК та позбавлений операції додавання двох точок ЕК, що значно зменшує обчислювальну складність процедури перевірки цифрового підпису. Крім того, в процедурі перевірки цифрового підпису зведено до мінімуму додаткові перетворення елементу поля і точки ЕК у велике ціле число.

Згідно з розглянутим методом, запропоновано відповідні алгоритми для його реалізації.

Формування загальносистемних параметрів може здійснюватись на основі відповідних алгоритмів, що використовуються у відомих стандартах ЦП, які базуються на математичному апараті ЕК. Так, наприклад, використовуючи ДСТУ 4145-2002 [8] степінь розширення поля m можна обрати відповідно до потрібного рівня криптостійкості з таблиці «Г.1 – Рекомендовані еліптичні криві в поліноміальному базисі» і відповідно до m обрати з цієї таблиці значення коефіцієнтів A, B еліптичної кривої E та n – порядок базової точки ЕК. Для обчислення базової точки еліптичної кривої P може використовуватись алгоритм «7.3 Обчислення базової точки еліптичної кривої», для вибору таємного ключа d може використовуватись алгоритм «9.1 Обчислення особистого ключа цифрового підпису», вибір тимчасового таємного ключа k може здійснюватись за алгоритмом «6.3 Обчислення випадкового цілого числа», для обчислення відкритого ключа Q може використовуватись алгоритм «9.2 Обчислення відкритого ключа цифрового підпису».

Функцію гешування H та генератор псевдовипадкових послідовностей для використання у запропонованому методі можна обирати згідно з відповідними державними стандартами або будь-якими іншими, рекомендованими в установленому порядку.

Процедуру формування цифрового підпису згідно з запропонованим методом належить здійснювати за алгоритмом 1.

Алгоритм 1 – Формування цифрового підпису згідно з запропонованим методом

Крок 1. *Обчислити геш-код на основі відкритого повідомлення* M: $h = H(M)$.

Крок 2. *Вибрати таємне випадкове велике ціле число* k.

Крок 3. *Обчислити точку ЕК:* $R = kP$.

Крок 4. *Обчислити елемент скінченого поля* $x_R = \lambda(R)$.

Крок 5. *Обчислити елемент скінченого поля вигляду* $\pi(h)x_R$ *та перетворити його на велике ціле число:*

$$r = \lambda(\pi(h)x_R) \bmod n.$$

Крок 6. *Обчислити велике ціле число* $z = dr \bmod n$.

Крок 7. *Обчислити точку ЕК вигляду* $L = zP$ *та перетворити отриману точку на велике ціле число*

$$m' = \vartheta(\lambda(L)) \bmod n.$$

Крок 8. *Обчислити велике ціле число вигляду* $s = m'(r + h) \bmod n$.

Крок 9. *Перетворити множину цілих чисел* $\{s,r\}$ *на рядок вигляду* $DS = \{0 \| s \| 0 \| r\}$, де DS – *цифровий підпис.*

Процедуру перевірки підпису згідно з запропонованимметодом належить здійснювати за алгоритмом 2.

Алгоритм 2 – **Перевірка цифрового підпису згідно з запропонованим методом**

Крок 1. *Обчислити геш-код на основі відкритого повідомлення* M *:* $h = H(M)$.

Крок 2. *Перетворити цифровий підпис* DS *на множину цілих чисел* $\{s,r\}$.

Крок 3. *Обчислити точку ЕК вигляду* $L' = rQ$ *та перетворити отриману точку на ціле число* $m'' = \vartheta(\lambda(L)) \bmod n$.

Крок 4. *Обчислити велике ціле число вигляду* $r' = (s - m''h') \bmod n$.

Крок 5. *Обчислити велике ціле число вигляду* $r'' = (rm'') \bmod n$.

Крок 6. *Перевірити: якщо* $r' \equiv r''$, *то підпис* DS *вважати вірним.*

Під час реалізації алгоритмів обов'язково потрібно враховувати приведення результатів обчислень над цілими числами за модулем n – порядку базової точки ЕК, а також результатів перетворення елементів скінченого поля і/або точок ЕК у велике ціле число.

Здійснено програмну реалізацію запропонованого методу, використовуючи бібліотеки математичних процедур та функції пакету BorZoi [9].

IV Порівняльний аналіз обчислювальної складності запропонованого методу цифрового підписування та ДСТУ 4145-2002

Для порівняння запропонованого методу ЦП із відомим методом ДСТУ 4145-2002 поставлено у відповідність кроки обчислень у вигляді, наведеному в таблиці 3. З таблиці 3 видно, що основними відмінностями запропонованого методу від ДСТУ 4145-2002 в процедурі перевірки є відсутність перетворення геш-коду в елемент скінченого поля, а в процедурі формування – наявність додаткової операції скалярного множення цілих чисел на точку ЕК вигляду zP. Також в процедурі перевірки відсутні одна операція скалярного множення точки ЕК на велике ціле число та операція додавання двох точок ЕК. Виходячи з цього, запропонований метод ЦП, порівняно з існуючими, має меншу обчислювальну складність процедури перевірки цифрового підпису за рахунок більш складної процедури формування.

Таблиця 3 – Порівняння послідовності обчислень згідно з запропонованим методом та ДСТУ 4145-2002

ДСТУ 4145-2002	Запропонований метод
Формування цифрового підпису	
$Q = -dP$	$Q = dP$
$h = \pi(H(M))$	$h = H(M)$
$R = eP,$ $y = h\lambda(R) = hx_R,$ $r = \vartheta(y) \bmod n$	$R = kP, x_R = \lambda(R), r = \vartheta(\pi(h)x_R) \bmod n$ $z = dr \bmod n$ $L = zP, x_L = \lambda(L), m' = \vartheta(x_L) \bmod n$
$s = (e + dr) \bmod n$	$s = m'(r + h) \bmod n$
$DS = \{0 \| r \| 0 \| s\}$	$DS = \{0 \| r \| 0 \| s\}$
Перевірка цифрового підпису	
$h' = \pi(H(M))$	$h' = H(M)$
$\{0 \| r \| 0 \| s\} = DS$	$\{0 \| r \| 0 \| s\} = DS$
$R' = sP + rQ,$ $y = h'\lambda(R') = h'x_R,$ $r' = \vartheta(y) \bmod n$	$L' = rQ, x'_L = \lambda(L'), m'' = \vartheta(x'_L) \bmod n$ $r' = (s - m''h') \bmod n$ $r'' = rm'' \bmod n$
Якщо $r \equiv r'$, то цифровий підпис вірний	Якщо $r' \equiv r''$, то цифровий підпис вірний

Для оцінювання часу виконання процедур формування/перевірки цифрового підпису та коректності функціонування запропонованого методу було здійснено його програмну реалізацію, а також програмну реалізацію ДСТУ 4145-2002 з метою проведення порівняння цих методів. Проведено перевірку запропонованого методу ЦП та ДСТУ 4145-2002 для ключів довжин 163, 283, 409, 571 та відповідних ЕК, рекомендованих NIST [10]. Обчислення проводились в поліноміальному базисі [4, 8].

Приклад результатів роботи процедур ЦП на кожному обчислювальному кроці згідно з запропонованим методом та ДСТУ 4145-2002 для довжини ключа 163 біти наведено в табл. 4.

Таблиця 4 – Приклад результатів обчислень згідно запропонованого методу ЦП та ДСТУ 4145-2002

ДСТУ 4145-2002	Запропонований метод
Формування загальносистемних параметрів	
m = 163 $E: y^2 + xy = x^3 + Ax^2 + B$, A = 020a601907b8c953ca1481eb10512f78744a3205fd n = 040000000000000000000292fe77e70c12a4234c33 $P(x, y)$ = (03f0eba16286a2d57ea0991168d4994637e8343e36, d51fbc6c71a0094fa2cdd545b11c5c0c797324f1)	
Формування цифрового підпису	
d = 0326bd1857fe02fd147f7ea99abf2be8fc18ad1a34	d = 024d774541f52ab8a83f6b94b9264c016db93a0f5b
$Q(x, y)$ =(001b1bce071803abddd9b6f3bb283b31ee6645413f, 0119211a0903016a17cec2236063f19892988f4904	$Q(x, y)$ =0038d5d49194e4900469cab46279d3a1b539a2619a, 00b0a126b9d48e7dc0ec5874a4a64ed81084bb9b60
h = 6152ecd10857b27f7591b68a691e3eabc3919350	h = 6152ecd10857b27f7591b68a691e3eabc3919350
x_R = 0607dc910cd5ec6f40406d4c20a32c21c19f54ab97	x_R = 140b4d0399bff5de2e903d2f2e9e43e93151c497
$DS = \{0 \| s \| 0 \| r\}$ =0035d8af0a256c03b82c375f5d64d849972e46002d500112eb6f23af76f7b07e270d6ff6ab117f31099ca8	$DS = \{0 \| s \| 0 \| r\}$ =002ace0f37a7804ec36118ef7b252abbe2da0b15bbf00348bc70925e45a712064511b02709da0cb21f2471
Перевірка цифрового підпису	
h = 6152ecd10857b27f7591b68a691e3eabc3919350	h = 6152ecd10857b27f7591b68a691e3eabc3919350
$DS = \{0 \| s \| 0 \| r\}$ =0035d8af0a256c03b82c375f5d64d849972e46002d500112eb6f23af76f7b07e270d6ff6ab117f31099ca8	$DS = \{0 \| s \| 0 \| r\}$ =002ace0f37a7804ec36118ef7b252abbe2da0b15bbf00348bc70925e45a712064511b02709da0cb21f2471
$\lambda(sP)$ = 029a1aa0cb7f124d296ccef9cb03035f648260c597 $\lambda(rQ)$ = 05243a9b1d1a95dece099e33018ca2f3d39373d358 R' = 0607dc910cd5ec6f40406d4c20a32c21c19f54ab97 r' = 0112eb6f23af76f7b07e270d6ff6ab117f31099ca8	rQ(x, y) = 04a77c13719be56e375b9662a17e3adcdd8633804a, 0159629eed84097400515f9dd1e344f05cfcb56b73) m' = 02803386dddc3a7ea16268055300a6c22189014b6e r' = e1f5f3dc9836d9f0391d765433e187c0140a8706 R'' = e1f5f3dc9836d9f0391d765433e187c0140a8706
$r \equiv r'$ – підпис вірний	$r' \equiv r''$ – підпис вірний

Результати аналізу часу виконання процедур формування та перевірки цифрового підпису для різних довжин ключів згідно з запропонованим методом ЦП та ДСТУ 4145-2002 представлено в табл. 5.

Таблиця 5 – Порівняння часу формування/перевірки підпису згідно запропонованого методу та відомого ДСТУ 4145-2002

Довжина ключа, біт	Час виконання процесу формування цифрового підпису, мілісекунд		Час виконання процесу перевірки цифрового підпису, мілісекунд	
	ДСТУ 4145-2002	Запропонований метод	ДСТУ 4145-2002	Запропонований метод
163	199	376	391	183
283	679	1335	1340	619
409	1525	3128	3180	1515
571	3371	7044	6952	3500

З табл. 5 видно, що процедура перевірки цифрового підпису згідно з запропонованим методом виконується значно швидше за процедуру перевірки підпису, ніж в ДСТУ 4145-2002, але при цьому процедура підписування за запропонованим методом виконується довше, ніж за ДСТУ 4145-2002. Співвідношення формування/перевірка цифрового підпису для запропонованого методу в середньому 1:2.1, а для ДСТУ 4145-2002 – 2:1.

Також аналіз результатів табл. 5 показує, що в запропонованому методі цифрового підписування процедура перевірки цифрового підпису потребує приблизно від 70% до 100% менше часу для перевірки,

ніж ДСТУ 4145-2002. При цьому, на формування підпису витрачається від 60% до 90% більше часу, ніж ДСТУ 4145-2002.

V Аналіз криптостійкості запропонованого методу цифрового підписування

Проаналізуємо запропонований метод з точки зору теоретичної криптостійкості.

При цьому будемо враховувати, що як зловмисник може виступати як третя сторона, так і будь-який санкціонований користувач криптосистеми.

Спочатку слід врахувати, що зловмиснику відомі такі загальносистемні параметри: m - степінь розширення основного поля; ЕК задана рівнянням (13), n – порядок базової точки ЕК; P – базова точка ЕК; Q – відкритий ключ; H – обрана функція гешування. Також відомий сам цифровий підпис у вигляді великих цілих чисел $\{s, r\}$.

Для обчислення цифрового підпису або підробки повідомлення M, зловмиснику, згідно з виразами (5) та (6) потрібно обчислити значення r та s. Як видно з виразів (7) та (10) обчислення невідомих великих цілих чисел m' та x_R можливе тільки при вирішенні задачі дискретного логарифмування в групі точок ЕК для шуканих великих цілих.

Розглянемо можливість підробки підпису у випадку, коли зловмисник має відкритий ключ Q і може отримувати обчислені значення кожного кроку перевірки цифрових підписів з множини $\{DS_0, DS_1,..., DS_v\} \in \{\{s_0, r_0\}, \{s_1, r_1\},..., \{s_v, r_v\}\}$ та відповідних їм повідомлень $\{M_0, M_1,..., M_v\}$, де v – кількість підписаних повідомлень. В цьому випадку будемо вважати, що всі загальносистемні параметри при підписуванні цих повідомлень будуть однаковими. Тоді, зловмисник може отримати під час перевірки підписів множину таємних цілих чисел

$$\{m'_0, m'_1,..., m'_v\} \in \{m''_0, m''_1,..., m''_v\} \in \{\vartheta(\lambda(r_0 Q)), \vartheta(\lambda(r_1 Q)),..., \vartheta(\lambda(r_v Q))\}, \quad (14)$$

що дає йому можливість обчислити цілі числа з множини

$$\{s_0, s_1,..., s_v\} \in \{m''_0(r_0 + h_0) \bmod n, m''_1(r_1 + h_1) \bmod n,..., m''_v(r_v + h_v) \bmod n\}. \quad (15)$$

Однак, цього не достатньо для формування цифрових підписів DS_i, $i = \overline{0, v}$, оскільки з врахуванням виразів (9) та (12), $m'_0 \neq m'_1 \neq ... \neq m'_v$ і, відповідно $m''_0 \neq m''_1 \neq ... \neq m''_v$, але за умови, що $M_0 \neq M_1 \neq ... \neq M_v$. Таким чином, знаючи множину повідомлень, зловмисник має можливість обчислити тимчасові таємні ключі $m'_i \equiv m''_i$ та цілі числа s_i, але не має можливості обчислити цілі числа r_i і підробити підпис DS_i для відповідного повідомлення, а також будь-якого іншого повідомлення M_i із множини повідомлень. Також, слід зазначити, що зловмисник на основі відомих йому даних може сформувати множину цілих $\{s_0, s_1,..., s_v\}$ тільки для множини повідомлень $\{M_0, M_1,..., M_v\}$, і не більше.

Якщо зловмисник спробує знайти тимчасовий таємний ключ k та цілі числа множини $\{s_0, s_1,..., s_v\}$, що обчислюються відповідно до $\{\vartheta(\pi(h_0) x_R) \bmod n, \vartheta(\pi(h_1) x_R) \bmod n,..., \vartheta(\pi(h_v) x_R) \bmod n\}$ та $\{r_0, r_1,..., r_v\}$, які в свою чергу, обчислюються відповідно до

$$\{'m_0(r_0 + h_0) \bmod n, m'_1(r_1 + h_1) \bmod n,..., m'_v(r_v + h_v) \bmod n\}, \quad (16)$$

то йому потрібно буде визначити цілі числа з множини

$$\{z_0, z_1,..., z_v\} \in \{dr_0 \bmod n, dr_1 \bmod n,..., dr_v \bmod n\}. \quad (17)$$

Тоді для обчислення

$$\{m'_0, m'_1,..., m'_v\} \in \{\vartheta(\lambda(z_0 \mathrm{P})), \vartheta(\lambda(z_1 \mathrm{P})),..., \vartheta(\lambda(z_v \mathrm{P}))\} \quad (18)$$

та цілого числа k, яке необхідно для обчислення елементу скінченого поля $x_R = \lambda(kP)$ і підробки повідомлення M довільного вигляду, потрібно розв'язати задачу дискретного логарифмування в групі точок ЕК.Слід також відзначити, що з виразів (2), (3) та (4), а також з виразів (5) та (6) зловмисник має можливість обчислити значення таємного цілого числа d тільки у випадку, якщо буде розв'язана задача дискретного логарифмування в групі точок ЕК.

Ще однією дією зловмисника може бути спроба обчислення колізій для функції гешування H,якщо

геш-код обчислюється як $h=H(M)$. Для попередження можливості попереднього обчислення колізій функції гешування потрібно здійснити заміщення виразу $h = H(M)$ виразом вигляду $h = H(M \| m')$, де m' – ціле число, яке обчислено на основі таємного ключа.

Отже розглянуті спроби зламу зводяться до вирішення задачі дискретного логарифмування в групі точок ЕК. На основі проведеного аналізу криптостійкості запропонованого методу ЦП можна зробити висновок, що метод є достатньо криптостійким.

VI Висновки

Запропоновано метод ЦП на основі математичного апарату ЕК, який дозволив прискорити процес перевірки цифрового підпису за рахунок перенесення операції скалярного добутку великого цілого числа на базову точку ЕК з процедури перевірки цифрового підпису в процедуру формування та введенням в ці процедури додаткових обчислень над великими цілими числами за модулем порядку базової точки.

Здійснено програмну реалізацію запропонованого методу, проведено порівняльний аналіз часу формування/перевірки підпису за даним та відомим методом ЦП. Запропонований метод ЦП має приблизно на 70% більш швидку процедуру перевірки підпису порівняно з відомими методами ЦП на основі ЕК. Це забезпечується за рахунок менш швидкої (на 60 %) процедури формування підпису.

Таким чином, запропонований метод дозволив підвищити швидкість перевірки цифрового підпису порівняно з відомими методами, що в свою чергу, дозволяє вирішувати проблему перевантаження процедури перевірки підпису в задачах, де ця проблема є критичною.

Дослідження криптостійкості запропонованого методу показало, що спроби його зламу зводяться до необхідності вирішення задачі дискретного логарифмування в групі точок ЕК.

Література: ***1.*** *Menezes A. J., van Oorschot P. C., Vanstone S. A. Handbook of Applied Cryptography. CRC Press, 1996.* ***2.*** *Miller V. S. Use of Elliptic Curves in Cryptography// Advances in Cryptology - Crypto'85. LNCS 218, - 1986, p. 417 - 426.* ***3.*** *Болотов А. А., Машков С. Б., Фролов А. Б., Часовских А. А. Элементарное введение в эллиптическую криптографию. Алгебраические и алгоритмические основы. - М.: КомКнига, 2006. - 328 с.* ***4.*** *Бессалов А. В., Телиженко А. Б. Криптосистемы на эллиптических кривых: Учеб. Пособие. – К.: ІОЦ «Видавництво «Політехніка», 2004. – 224 с.: іл.* ***5.*** *Adrian Antipa, Daniel R. L. Brown, Robert P. Gallant, Robert J. Lambert, Rene Struik, Scott Vanstone. "Accelerated Verification of ECDSA Signatures". Certicom Research, Canada, 2005: p. 307-318.* ***6.*** *Пат. EP1306750 JP, МКИ G09C1/00; G06F7/72; G09C1/00; G06F7/60; (IPC1-7): G06F7/72. "Multi-scalar multiplication computation in elliptic curve signature verification": Пат. EP1306750, МКИ G06F7/72F1. // Okeya Katsuyuki (JP) - № EP20020255073; Заявл. 19.07.2002; Опубл. 02. 05. 2003.* ***7.*** *Пат. US2007064932 CA, МКИ H04L9/30; H04L9/28. "Accelerated verification of digital signatures and public keys" // Struik Marinus; Brown Daniel; Vanstone Scott; Gallant Robert; Antipa Adrian; Lambert Robert - №US20060333296. Заявл. 18. 01. 2006; Опубл. 22. 03. 2007.* ***8.*** *ДСТУ 4145-2002. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. - К.: Держстандарт України, 2003. – 94 с.* ***9.*** *Anthony Mulcahy. BorZoi - An Elliptic Curve Cryptography Library // Available at http://dragongate-technologies.com/products.html.*

УДК 681.528.54

ВИКОРИСТАННЯ МАТЕМАТИЧНОГО АПАРАТУ НЕЧІТКИХ МНОЖИН ДЛЯ РОЗРОБКИ МЕТОДІВ, ТЕХНОЛОГІЙ, МОДЕЛЕЙ СИСТЕМ БЕЗПЕКИ ІНФОРМАЦІЇ

Валерій Домарєв
Апарат РНБО України

Анотація: **Викладено питання розроблення методів, технологій, моделей і систем безпеки інформації, які з використанням математичного апарату нечітких множин дозволяють ефективно впроваджувати захищені інформаційні технології.**
Summary: **The subjects of methods, technologies, models and information security systems development are presented, which with the use of mathematical fuzzy sets apparatus allow effective introduction of the protected information technologies.**
Ключові слова: **Методи, технології, моделі систем безпеки інформації.**