

2 Забезпечення комп'ютерної безпеки в державних, банківських та інших інформаційних системах

УДК 621.391.7

МЕТОД ПРИСКОРЕНОГО ЦИФРОВОГО ПІДПISУВАННЯ НА ОСНОВІ МАТЕМАТИЧНОГО АПАРАТУ ЕЛІПТИЧНИХ КРИВИХ

Юрій Яремчук, Костянтин Черняхович

Вінницький національний технічний університет

Анотація: Запропоновано метод цифрового підписування на основі математичного апарату еліптичних кривих, який дозволяє прискорити цифрове підписування порівняно з відомими аналогами.

Summary: This work proposes the method of digital signing based on the mathematical background of elliptic curves which allows to accelerate digital signing in comparison with known prototypes.

Ключові слова: захист інформації, криптографія, цифрове підписування, еліптичні криві.

І Вступ. Постановка задачі

Проблема цифрового підписування (ЦП) ефективно вирішується за допомогою методів на основі математичного апарату еліптичних кривих (ЕК), до яких, зокрема, відносяться ECDSA, ECSS та ін. [1 – 3]. Ці методи порівняно зі своїми попередниками (RSA, DSA та ін. [4]) дозволяють при забезпеченні достатнього рівня криптостійкості використовувати значно менші ключі та загальносистемні параметри.

Однак, на практиці існує ряд прикладних задач, в яких перевірку цифрового підпису необхідно здійснювати значно частіше, ніж його формування. До таких задач в першу чергу відносять задачі безпеки банківських трансакцій, електронного документообігу, електронних платіжних систем, електронної (e-commerce) та мобільної комерції (m-commerce), підписування повідомлень електронної пошти та ін. В цьому випадку складна процедура перевірки цифрового підпису може призводити до перевантаження системи, що реалізує певну вищевказану прикладну задачу.

Для вирішення цієї проблеми в роботах [5 – 7], на прикладі ECDSA, запропоновано модифікації з прискореною процедурою перевірки цифрового підпису за рахунок використання передобчислень. Однак, ці модифікації не забезпечують суттєвого прискорення перевірок цифрового підпису і вимагають використання пам'яті системи ЦП для зберігання результатів передобчислень.

В роботі [8] запропоновано метод ЦП з прискореною процедурою перевірки цифрового підпису. Суть методу полягає в перенесенні операції скалярного добутку великого цілого числа на базову точку ЕК з процедури перевірки підпису в процедуру формування. Однак, при цьому суттєво збільшується обчислювальна складність процедури формування підпису, і як наслідок, часу виконання цієї процедури.

В зв'язку з цим, актуальними є дослідження, спрямовані на підвищення швидкості перевірки цифрового підпису та розробку методів ЦП на основі математичного апарату ЕК з прискореною процедурою перевірки цифрового підпису без застосування попередніх обчислень, а також компенсації зменшення обчислювальної складності процедури перевірки за рахунок збільшення обчислювальної складності процедури формування підпису.

II Метод цифрового підписування на основі математичного апарату еліптичних кривих з прискореною процедурою перевірки підпису

Аналіз методів цифрового підписування на основі математичного апарату ЕК показав, що в процедурах формування підпису використовується операція скалярного добутку великого цілого числа на точку ЕК вигляду

$$R = kP, \quad (1)$$

а в процедурах перевірки підпису – сума скалярних добутків вигляду

$$R = sP + rQ, \quad (2)$$

де P – базова точка ЕК порядку n , що належить ЕК E ($P \in E$), заданій рівнянням вигляду $y^2 + xy = x^3 + Ax^2 + B$ (A, B – коефіцієнти рівняння); k – тимчасовий таємний ключ, як велике ціле

число; Q – відкритий ключ, як точка ЕК порядку n ; r та s – складові цифрового підпису, який перевіряється.

Тобто, з точки зору складності обчислень, в процедурі перевірки цифрового підпису використовується дві операції скалярного добутку великого цілого числа на точку ЕК, в той час як в процедурі формування підпису лише одна.

В зв'язку з цим пропонується метод на основі математичного апарату ЕК (заявка на корисну модель № u2007 11339 від 12. 10. 2007 р.), в якому для спрощення обчислювальної складності в процедурі перевірки цифрового підпису пропонується замість операції скалярного добутку великого цілого числа на базову точку $P \in E$ використовувати лише базову точку P . Тобто, на відміну від відомих методів ЦП на основі математичного апарату ЕК, замість виразу (2) в процедурі перевірки значення $R' \in E$ пропонується обчислювати за виразом

$$R' = m'Q - P, \quad (3)$$

де m' – велике ціле число, обчислене за формулою

$$m' = sh'^{-1} \bmod n, \quad (4)$$

де h' – обчислений геш-код у вигляді цілого числа від повідомлення M .

Використання виразів (3) та (4) замість (2) дозволяє зменшити обчислювальну складність процедур перевірки цифрового підпису, що приводить до прискорення перевірки цифрового підпису без збільшення обчислювальної складності процедури формування цифрового підпису.

Для забезпечення можливості перевірки цифрового підпису за виразами (3) та (4) в процедурі формування цифрового підпису обчислення s та r пропонується здійснювати за виразами

$$s = (k+1)hd^{-1} \bmod n, \quad (6)$$

$$r = \mathcal{G}(\pi(h)x_R) \bmod n, \quad (7)$$

де h – геш-код від повідомлення M , який обчислюється за допомогою функції гешування H у вигляді елементу скінченного поля; k – тимчасовий таємний ключ у вигляді великого випадкового цілого числа; x_R – елемент скінченного поля, який обчислюється за виразом вигляду $x_R = \lambda(R)$, де R – точка ЕК, яка обчислюється за виразом вигляду $R = kP$.

В процедурі перевірки цифрового підпису отримане значення великого цілого числа r пропонується порівнювати зі значенням великого цілого числа r' , що обчислюється за виразом

$$r' = \mathcal{G}(\lambda(R')\pi(h')) \bmod n, \quad (8)$$

де $\pi(\cdot)$ – функція перетворення великого цілого числа на елемент скінченного поля; $\mathcal{G}(\cdot)$ – функція перетворення елементу скінченного поля на ціле число;

$\lambda(\cdot)$ – функція перетворення точки ЕК в елемент скінченного поля.

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

Згідно з запропонованим методом, спочатку потрібно сформувати загальносистемні параметри, до яких слід віднести m – степінь розширення основного поля; еліптичну криву E ;

n – порядок базової точки ЕК; P – базову точку ЕК; d – таємний ключ, як велике ціле число; Q – відкритий ключ; k – тимчасовий таємний параметр, як випадкове велике ціле число; H – обрану функцію гешування.

Формування загальносистемних параметрів може здійснюватись на основі відповідних алгоритмів, які використовуються у відомих стандартах цифрового підписування, що базуються на математичному апараті ЕК.

Після того, як сформовано загальносистемні 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 $R \in E$. Обчислити велике ціле число r як добуток елементу скінченного поля у вигляді координати x точки $R \in E$ на попередньо перетворений в елемент скінченного поля геш-код h . Обчислити велике ціле число s як добуток гешу повідомлення h на обернене значення таємного ключа d , тобто d^{-1} ,

та перемножити отримане значення на ціле число $k+1$. Отриману пару цілих чисел $\{s, r\}$ перетворити на цифровий підпис вигляду $DS = (0 \parallel s \parallel 0 \parallel r)$.

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 вигляду M , використовуючи задану функцію гешування H . Перетворити цифровий підпис DS на пару цілих $\{s, r\}$. Обчислити значення m' як добуток великого цілого числа s на велике ціле число h'^{-1} . Обчислити точку $R' \in E$ як різницю базової точки $P \in E$ від скалярного добутку великого цілого числа m' на точку $Q \in E$. Обчислити ціле число r' як перетворений на велике ціле число добуток елементів скінченного поля $\lambda(R')$ на $\pi(h')$. Якщо отримане значення r дорівнює обчисленому r' , тобто $r \equiv r'$, то підпис вірний.

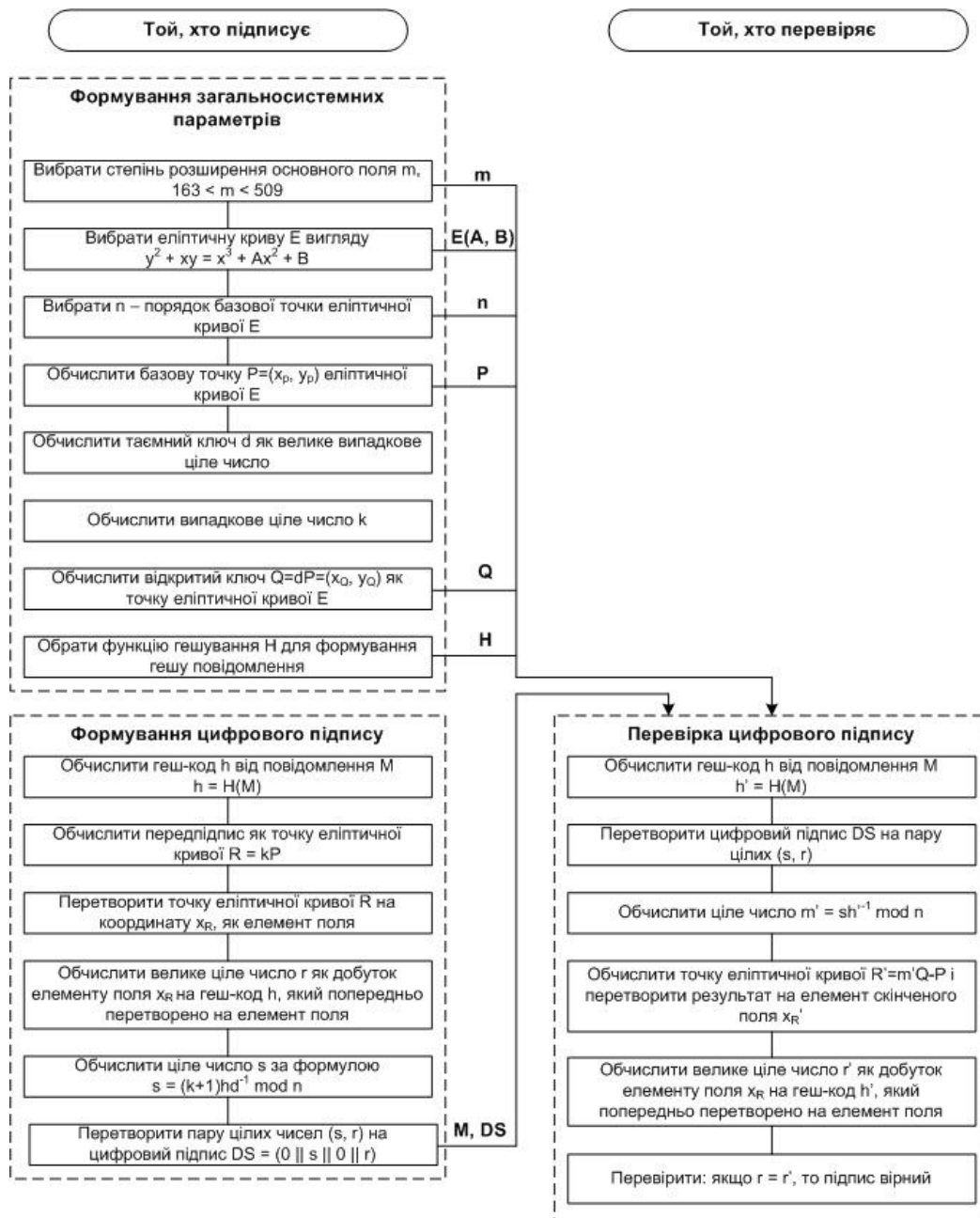


Рисунок 1 – Схема запропонованого методу прискореного ЦП на основі математичного апарату ЕК

Таким чином, запропоновано метод ЦП на основі математичного апарату ЕК, в якому в процедурі перевірки цифрового підпису використовується лише одна операція скалярного добутку великого цілого числа на точку ЕК, що значно зменшує обчислювальну складність процедури перевірки цифрового підпису.

Згідно з розглянутим методом, запропоновано відповідні алгоритми для його реалізації: для формування підпису – алгоритм 1, а для перевірки підпису – алгоритм 2.

Алгоритм 1 – Формування цифрового підпису згідно з запропонованим методом

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

Крок 2. Обчислити таємне випадкове велике ціле число k .

Крок 3. Обчислити передпідпис $R = kP$.

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

Крок 5. Обчислити елемент скінченного поля вигляду $\pi(h)x_R$ та перетворити його на велике ціле число: $r = \mathcal{G}(\pi(h)x_R) \bmod n$.

Крок 6. Обчислити велике ціле число вигляду $s = (k + 1)hd^{-1} \bmod n$.

Крок 7. Перетворити пару цілих чисел $\{s, r\}$ на цифровий підпис вигляду $DS = (0 \parallel s \parallel 0 \parallel r)$.

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 вигляду DS на пару цілих чисел $\{s, r\}$.

Крок 3. Обчислити велике ціле число $m' = sh'^{-1} \bmod n$.

Крок 4. Обчислити точку ЕК вигляду $R' = m'Q - P$.

Крок 5. Обчислити велике ціле число вигляду $r' = \mathcal{G}(\lambda(R')\pi(h')) \bmod n$.

Крок 6. Якщо $r \equiv r'$, то підпис вигляду DS вірний.

Здійснено програмну реалізацію запропонованого методу за розглянутими алгоритмами, використовуючи бібліотеки математичних процедур та функцій пакету BorZoi [9].

III Порівняльний аналіз часу виконання процедур формування/перевірки запропонованого методу цифрового підписування та ДСТУ 4145-2002

Для порівняння та наочного представлення запропонованого методу ЦП із відомим методом ДСТУ 4145-2002 [10] поставлено у відповідність кроки обчислень у вигляді, наведеному в таблиці 1.

Таблиця 1 – Порівняння послідовності обчислень згідно з запропонованим методом та ДСТУ 4145-2002

ДСТУ 4145-2002	Запропонований метод
Формування цифрового підпису	
$Q = -dP$	$Q = dP$
$h = \pi(H(M))$	$h = \pi(H(M))$
$R = eP,$ $y = h\lambda(R) = hx_R,$ $r = \mathcal{G}(y) \bmod n$	$R = kP,$ $y = h\lambda(R) = hx_R,$ $r = \mathcal{G}(y) \bmod n,$
$s = (e + dr) \bmod n$	$s = (k + 1)hd^{-1} \bmod n$
$DS = \{0 \parallel r \parallel 0 \parallel s\}$	$DS = \{0 \parallel s \parallel 0 \parallel r\}$
Перевірка цифрового підпису	
$h' = \pi(H(M))$	$h' = H(M)$
$\{0 \parallel r \parallel 0 \parallel s\} = DS$	$\{0 \parallel s \parallel 0 \parallel r\} = DS$
$R' = sP + rQ,$ $y = h'\lambda(R') = h'x_{R'},$ $r' = \mathcal{G}(y) \bmod n$	$m' = sh'^{-1} \bmod n,$ $R' = m'Q - P,$ $r' = \mathcal{G}(\lambda(R')\pi(h')) \bmod n$
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 [11]. Обчислення проводились в поліноміальному базисі [10].

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. 2.

Таблиця 2 – Приклад результатів обчислень згідно з запропонованим методом ЦП та ДСТУ 4145-2002

ДСТУ 4145-2002		Запропонований метод
Формування загальносистемних параметрів		
$m = 163$ $E : y^2 + xy = x^3 + Ax^2 + B, \quad A = 020\text{a}601907\text{b}8\text{c}953\text{ca}1481\text{eb}10512\text{f}78744\text{a}3205\text{fd}$ $n = 0400000000000000000000000292\text{fe}77\text{e}70\text{c}12\text{a}4234\text{c}33$ $P(x, y) = (03\text{f}0\text{eba}16286\text{a}2\text{d}57\text{ea}0991168\text{d}4994637\text{e}8343\text{e}36, \text{d}51\text{fb}\text{c}6\text{c}71\text{a}0094\text{fa}2\text{cd}\text{d}545\text{b}11\text{c}5\text{c}0\text{c}797324\text{f}1)$		
Формування цифрового підпису		
$d = 03125525\text{bd}5\text{eba}93\text{b}4915\text{fe}1\text{c}86\text{ff}35\text{d}30\text{baa}38\text{e}54$ $Q(x, y) = (040821057\text{eea}294\text{d}4\text{cbf}053\text{ae}7\text{bcff}7047\text{b}2315\text{a}8\text{b}, 009\text{bf}339\text{c}19\text{d}51414745\text{b}7678\text{b}19\text{fb}\text{d}912\text{b}2005317)$ $h = 6152\text{ecd}10857\text{b}27\text{f}7591\text{b}68\text{a}691\text{e}3\text{eabc}3919350$ $x_R = 02944\text{caf}3\text{eff}3516\text{af}28\text{a}64\text{ff}036\text{f}5685\text{b}31\text{db}09\text{a}5$		
$DS = \{0 \ s \ 0 \ r\} = 0035\text{d}8\text{af}0\text{a}256\text{c}03\text{b}82\text{c}375\text{f}5\text{d}64\text{d}849972\text{e}46002\text{d}500112\text{eb}6\text{f}23\text{af}76\text{f}7\text{b}07\text{e}270\text{d}6\text{ff}6\text{ab}117\text{f}31099\text{ca}8$	$DS = \{0 \ s \ 0 \ r\} = 08\text{f}062548\text{dca}7321\text{ba}3\text{c}88\text{ca}03981\text{afb}31\text{ac}951\text{a}600299\text{f}3\text{c}38\text{f}9\text{ed}181\text{f}8\text{fce}4\text{d}67679130\text{b}5\text{d}701\text{dadd}1$	
Перевірка цифрового підпису		
$h = 6152\text{ecd}10857\text{b}27\text{f}7591\text{b}68\text{a}691\text{e}3\text{eabc}3919350$ $DS = \{0 \ s \ 0 \ r\} = 002\text{c}5\text{af}3\text{f}2619\text{fd}9356\text{a}2\text{b}8\text{c}2\text{dc}7\text{f}919807405\text{ca}63700245298\text{e}67\text{db}87\text{a}003497\text{b}85\text{d}5739\text{f}17187107\text{f}269$ $\lambda(sP) = 03\text{b}47249\text{d}38\text{db}640\text{fff}7\text{fdb}0894\text{b}636\text{c}45\text{dd}005\text{afe}$ $\lambda(rQ) = 01\text{a}1\text{b}0\text{c}7\text{c}1\text{c}114\text{c}89167\text{be}2\text{b}46\text{f}5155\text{e}26\text{aac}63\text{a}12$ $x'_R = 02944\text{caf}3\text{eff}3516\text{af}28\text{a}64\text{ff}036\text{f}5685\text{b}31\text{db}09\text{a}5$ $r' = 0112\text{eb}6\text{f}23\text{af}76\text{f}7\text{b}07\text{e}270\text{d}6\text{ff}6\text{ab}117\text{f}31099\text{ca}8$		
$r \equiv r'$ – підпис вірний	$R' = (059\text{e}29\text{f}5200\text{f}53\text{f}60\text{b}4\text{d}5\text{ee}\text{f}37\text{fb}528\text{e}24\text{b}4\text{afbb}07, 03951\text{a}61\text{fb}1252\text{eec}3383898\text{acd}6\text{fb}8797168\text{f}74\text{fa})$ $x'_R = 059\text{e}29\text{f}5200\text{f}53\text{f}60\text{b}4\text{d}5\text{ee}\text{f}37\text{fb}528\text{e}24\text{b}4\text{afbb}07$ $r' = 0299\text{f}3\text{c}38\text{f}9\text{ed}181\text{f}8\text{fce}4\text{d}67679130\text{b}5\text{d}701\text{dadd}1$ $r \equiv r'$ – 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. 3.

Таблиця 3 – Порівняння часу формування/перевірки підпису згідно з запропонованим методом та відомого ДСТУ 4145-2002

Довжина ключа, біт	Час виконання процедури формування цифрового підпису, мілісекунд		Час виконання процедури перевірки цифрового підпису, мілісекунд	
	ДСТУ 4145-2002	Запропонований метод	ДСТУ 4145-2002	Запропонований метод
163	199	202	391	188
283	679	688	1340	671
409	1525	1547	3180	1526
571	3371	3453	6952	3559

З табл. 3 видно, що процедура перевірки цифрового підпису згідно з запропонованим методом виконується значно швидше за процедуру перевірки підпису, ніж в ДСТУ 4145-2002, при цьому процедура підписування за запропонованим методом не значно поступається ДСТУ 4145-2002. Співвідношення формування/перевірка цифрового підпису за запропонованим методом в середньому 1:1.03, а для ДСТУ 4145-2002 – 2:1.

Також аналіз результатів табл. 3 показує, що в запропонованому методі цифрового підписування процедура перевірки цифрового підпису потребує приблизно в 1,5-2 рази менше часу, ніж ДСТУ 4145-2002.

Якщо порівнювати швидкість виконання процедур формування та перевірки цифрового підпису запропонованого методу з результатами методу, запропонованого у роботі [12], то слід відзначити, що запропонований метод має в 2,04 рази більш швидку процедуру формування та лише в 1,01 рази повільнішу процедуру перевірки, ніж метод, розглянутий у роботі [12].

IV Аналіз криптостійкості запропонованого методу цифрового підписування

Проведемо аналіз запропонованого методу з точки зору теоретичної криптостійкості.

В разі виконання криптоаналізу запропонованого методу зломиснику будуть відомі такі загальносистемні параметри: m - степінь розширення основного поля; n - порядок базової точки ЕК; P - базова точка ЕК; Q - відкритий ключ; H - обрана функція гешування. Також відомий сам цифровий підпис $\{s, r\}$ у вигляді великих цілих чисел.

Для обчислення цифрового підпису вигляду $\{s, r\}$ для будь-якого повідомлення M зломиснику потрібно знати такі дані як d - таємний ключ, k - тимчасовий таємний ключ. При цьому, якщо зломисник спробує обчислити значення d , то йому потрібно буде розв'язати систему рівнянь з $i+1$ невідомими вигляду

$$\begin{cases} d = \left(\frac{(k_1 + 1)h_1}{s_1} \right) \bmod n, \\ \dots \\ d = \left(\frac{(k_i + 1)h_i}{s_i} \right) \bmod n. \end{cases} \quad (9)$$

Як видно з (9) значення k_i різне для кожного значення складових s_i та r_i цифрового підпису, тому обчислення значень k_i із системи вигляду

$$\begin{cases} k_1 = \left(\frac{s_1}{h_1 d^{-1}} - 1 \right) \bmod n, \\ \dots \\ k_i = \left(\frac{s_i}{h_i d^{-1}} - 1 \right) \bmod n \end{cases} \quad (10)$$

є практично не можливим, а обчислення тимчасового таємного параметра k із виразу вигляду (7) зводиться до вирішення задачі дискретного логарифмування в групі точок ЕК.

Слід відзначити, що криптостійкість запропонованого методу може бути підсилена у випадку завдання гешу у неявному вигляді. Це може бути досягнуто, наприклад, використанням замість виразу (6) виразу вигляду $s = (k + 1)rd^{-1} \bmod n$, тоді, замість виразу (4) потрібно використовувати вираз вигляду $m' = sr^{-1} \bmod n$. В цьому випадку система рівнянь (9) перетвориться на систему, яка буде мати $2i + 1$ невідомих.

Отже, розглянуті спроби зламу на теоретичному рівні зводяться до вирішення задачі дискретного логарифмування в групі точок ЕК або використання атак типу «груба сила» чи підбору ключів. Зазвичай такі види атак не є ефективними при правильно обраних таємних ключах та загальносистемних параметрах. На основі проведеного аналізу криптостійкості запропонованого методу ЦП можна зробити висновок, що метод є достатньо криптостійким.

V Висновки

Запропоновано метод ЦП на основі математичного апарату ЕК, який дозволяє суттєво зменшити обчислювальну складність процедури перевірки цифрового підпису при не значному збільшенні обчислювальної складності процедури формування цифрового підпису відносно відомих методів.

Прискорення досягається за рахунок того, що в процедурі перевірки підпису при обчисленні контрольної складової цифрового підпису замість операції скалярного добутку великого цілого числа на базову точку $P \in E$ використовується лише сама базова точка P . При цьому показано, що рівень криптостійкості запропонованого методу не зменшився порівняно з відомим.

Здійснено програмну реалізацію запропонованого методу, а також проведено порівняльний аналіз часу формування/перевірки підпису за даним та відомим методом ЦП. Запропонований метод ЦП має приблизно в 1,5-2 рази більш швидко процедуру перевірки підпису порівняно з відомими методами ЦП на основі ЕК.

Таким чином, запропонований метод дозволив підвищити швидкість перевірки цифрового підпису порівняно з відомими методами.

Література: 1. ANSI X9.62-1999. Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA). – 1999. 2. Болотов А. А., Машиков С. Б., Фролов А. Б., Часовских А. А. Элементарное введение в эллиптическую криптографию. Алгебраические и алгоритмические основы. – М.: КомКнига, 2006. – 328 с. 3. Беспалов А. В., Телиженко А. Б. Криптосистемы на эллиптических кривых: Учеб. Пособие. – К.: ИОЦ «Видавництво «Політехніка», 2004. – 224 с.: іл. 4. Menezes A. J., van Oorschot P. C., Vanstone S. A. Handbook of Applied Cryptography. CRC Press, 1996. 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. Пат. UA24459, МПК(2006) H03M 13/00. «Способ цифрового подписывания на основе математического аппарата эллиптических кривых» // Яремчик Ю. С.; Черняхович К. В. - № U200705052. Заявл. 07.05.2007; Опубл. 25.06.2007, Бюл. №9, 2007. 9. Anthony Mulcahy. BorZoi – An Elliptic Curve Cryptography Library // Available at <http://dragongate-technologies.com/products.html>. 10. ДСТУ 4145-2002. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. – К.: Держстандарт України, 2003. – 94 с. 11. Standards for Efficient Cryptography Group. SEC 2: Recommended Elliptic Curve Domain Parameters, September 2000. Version 1.0. Available at www.secg.org. 12. Яремчик Ю. С., Черняхович К. В. Метод цифрового підписування на основі математичного апарату еліптичних кривих з прискореною процедурою перевірки підпису. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – К., 2007. – №1 (14), – С. 119 – 127.

УДК 681.31

ДОСЛІДЖЕННЯ МЕТОДІВ ЗАВАДОСТІЙКОГО КОДУВАННЯ ДЛЯ АВТОМАТИЗАЦІЇ ВИЗНАЧЕННЯ КОГНІТИВНИХ ВЛАСТИВОСТЕЙ ІНФОРМАЦІЇ

Сергій Троценко

Кафедра СКС ФПМ НТУУ "КПІ"

Анотація: Розглядається можливість застосування принципів завадостійкого кодування для визначення такої когнітивної властивості інформації, як її оригінальність. Приводяться визначення основних понять та постановка проблеми. Розглядається можливість порівняння послідовностей на основі принципів завадостійкого кодування, та їх застосування для визначення кількісних характеристик оригінальності інформації та пошуку запозичень.

Summary: The possibility of application of principles of error control codes for definition such cognitive properties of the information, as its originality is considered in this article. Definitions of the basic concepts and statement of a problem are given. The possibility of comparison of sequences on the basis of the error control codes, and also their application for definition of quantitative characteristics of originality of the information and search of loans is considered.

Ключові слова: Захист інформації, оригінальність інформації, завадостійке кодування.

В межах такої предметної області як інформатика інформацією називають відповідним чином упорядковану в результаті аналітико-синтетичної обробки множину даних, відомостей, знань, у тому числі комп'ютерних програм, які використовуються в автоматизованих системах (АС) незалежно від способу їх