УДК 519.1

Нікуліщев Г. І.

Старший викладач, Запорізький національний технічний університет, Україна, E-mail: tymahod@ukr.net

ПРОТОКОЛ СЛІПОГО ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ НА ЕЛІПТИЧНИХ КРИВИХ НАД СКІНЧЕНИМ ВЕКТОРНИМ ПОЛЕМ

У даній статті пропонується реалізація протоколу сліпого електронного цифрового підпису, що являє собою модифікацію стандарту ГОСТ Р 34.10-2001 на еліптичних кривих над скінченим векторним полем. Аналізується захищеність запропонованого протоколу за критерієм анонімності.

Ключові слова: сліпий електронний цифровий підпис, скінчене векторне поле, еліптична крива.

ВСТУП

Останнім часом особливої актуальності набуло питання забезпечення чесності та прозорості процедури виборів. У зв'язку з цим пильної уваги наукової спільноти набули механізми електронного голосування. Одним з методів реалізації такого механізму є використання сліпого електронного цифрового підпису (ЕЦП). Оскільки на разі схеми сліпого ЕЦП не стандартизовані, широко використовуються як власноручно розроблені схеми, так і модифікації існуючих стандартів.

В статті розглядається модифікація російського стандарту ЕЦП ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки ЭЦП». Цей стандарт базується на математичному апараті еліптичних кривих (ЕК) над простим полем Галуа. Для забезпечення необхідної криптостійкості стандартом рекомендується використовувати параметри алгоритму розміром 256 біт і вище, що зобумовлює достатню складність групової операції в групі точок ЕК. Як варіант оптимізації групової операції можна розглядати використання ЕК над скінченим векторним полем (СВП), яке дозволяє зберегти необхідний порядок групи точок ЕК при меншому розмірі елементів поля [1].

Сліпий ЕЦП вирішує специфічну задачу підтвердження справжності документів без розкриття їхнього авторства і, завдяки цьому, може використовуватись в схемах електронного голосування. В алгоритмі сліпого ЕЦП один учасник формує документ, а інший підписує його всліпу без можливості ознайомитися із вмістом. При цьому важливо, щоб навіть підписувач не зміг встановити автора документа. Через це до інших критеріїв захищеності схем ЕЦП у випадку сліпого підпису додається критерій анонімності. Він показує неможливість визначити автора документа з боку підписувача, якщо він використовуватиме всі відомі йому параметри, які використовувались при постановці підпису.

1 ЕЛІПТИЧНІ КРИВІ НАД СКІНЧЕНИМ ВЕКТОРНИМ ПОЛЕМ

Розглянемо одне з можливих розширень поля Галуа $GF(p)$ – скінчене векторне поле. В СВП входять вектори певної довжини n

$$v = v_1 \cdot e_1 + v_2 \cdot e_2 + ... + v_n \cdot e_n = (v_1, v_2, ..., v_n), \quad (1)$$

де $v_i \in GF(p)$, e_i – базисні вектори, $i = 1, 2, ..., n$.

На множині векторів визначимо операції додавання та множення.

Додавання двох векторів $u = (u_1, u_2, ..., u_n)$ та $v = (v_1, v_2, ..., v_n)$ відбувається за формулою

$$w = u + v = (u_1 + v_1 \bmod p, u_2 + v_2 \bmod p, ..., u_n + v_n \bmod p). \quad (2)$$

Одиничним елементом за операцією додавання є вектор $u_0 = (0, 0, ..., 0)$. Відповідно, вектор $u = (u_1, u_2, ..., u_n)$ називається оберненим до вектора $v = (v_1, v_2, ..., v_n)$, якщо $u + v = u_0$, тобто

$$v = -u = (-u_1 \bmod p, -u_2 \bmod p, ..., -u_n \bmod p). \quad (3)$$

Множення вектора v на число k реалізується за формулою

$$k \cdot a = (k \cdot a_1 \bmod p, k \cdot a_2 \bmod p, ..., k \cdot a_n \bmod p). \quad (4)$$

Позначимо операцію множення двох векторів знаком $\circ\!\!\%$. Ця групова операція мультиплікативної групи СВП визначається асоціативною таблицею множення базисних векторів [1], коефіцієнти перемножуються за принципом множення многочленів. В якості одиничного елемента СВП оберемо, наприклад, вектор $v_0 = (1, 0, ..., 0)$. Відповідно, два елементи СВП, результатом множення яких між собою є одиничний елемент, називаються взаємно оберненими.

Проілюструємо правило множення базисних векторів для довжини вектора $n = 2$ за допомогою табл. 1, для $n = 3$ – табл. 2. Значення розтягуючих коефіцієнтів τ і μ обчислюються з системи характеристичних рівнянь, що задає існування оберненого вектора для будь-якого заданого v.

Таблиця 1. Множення базисних векторів СВП для $n = 2$

$\circ$	e_1	e_2
e_1	e_1	e_2
e_2	e_2	$\tau \cdot e_2$

Таблиця 2. Множення базисних векторів СВП для $n = 3$

$\circ$	e_1	e_2	e_3
e_1	e_1	e_2	e_3
e_2	e_2	$\tau \cdot e_3$	$\tau \cdot \mu \cdot e_1$
e_3	e_3	$\tau \cdot \mu \cdot e_1$	$\mu \cdot e_2$

Відповідно до табл.1 система характеристичних рівнянь для $n = 2$ має вигляд

$$\begin{aligned} v_1 \cdot x + \tau \cdot v_2 \cdot y &= 1 \bmod p, \\ v_2 \cdot x + v_1 \cdot y &= 0 \bmod p. \end{aligned} \tag{5}$$

Якщо визначник $\Delta = {v_1}^2 - \tau \cdot {v_2}^2 \bmod p$ системи (5) приймає нульове значення, то для вектора $v = (v_1, v_2)$ не існує оберненого. Звідси, τ має бути квадратичним незалишком за модулем p. Тоді всі ненульові вектори СВП будуть утворювати мультиплікативну групу порядку $(p^2 - 1)$.

Відповідно до табл. 2 система характеристичних рівнянь для n=3 має вигляд

$$\begin{aligned} v_1 \cdot x + \tau \cdot \mu \cdot v_3 \cdot y + \tau \cdot \mu \cdot v_2 \cdot z &= 1 \bmod p, \\ v_2 \cdot x + v_1 \cdot y + \mu \cdot v_3 \cdot z &= 0 \bmod p, \\ v_3 \cdot x + \tau \cdot v_2 \cdot y + v_1 \cdot z &= 0 \bmod p. \end{aligned} \tag{6}$$

Якщо визначник системи (6) приймає нульове значення, то для вектора $v = (v_1, v_2, v_3)$ не існує оберненого. Величина $(p - 1)$ має ділитися на 3, а кожен з добутків $\tau^2 \cdot \mu$ та $\tau \cdot \mu^2$ має бути кубічним незалишком за модулем p. Тоді всі ненульові вектори СВП будуть утворювати мультиплікативну групу порядку $(p^3 - 1)$.

Розглянемо визначення ЕК над СВП. Оскільки характеристика СВП дорівнює p, то для $p \neq 2$ та $p \neq 3$ рівняння кривої можна записувати в скороченій формі

$$y \circ y = x \circ x \circ x + a \circ x + b, \tag{7}$$

де x, y, a, b – елементи СВП.

Кожна пара векторів x, y, що задовольняє рівнянню (7), вважається точкою ЕК. Сукупність всіх точок ЕК разом з нескінченно віддаленою точкою O складає групу точок ЕК над СВП.

Групова операція додавання точок ЕК над СВП визначається аналогічно до групової операції додавання точок ЕК над простим полем [2] з використанням операції множення векторів $\circ$. Координати точки $U = (x^U, y^U)$, яка представляє собою суму точок $S = (x^S, y^S)$ та $T = (x^T, y^T)$, визначаються за формулами

$$x^U = \lambda \circ \lambda - x^S - x^T, \tag{8}$$

$$y^U = \lambda \circ (x^S - x^U) - y^S. \tag{9}$$

Величина λ обчислюється за формулою (10), якщо $S \neq T$

$$\lambda = \frac{y^T - y^S}{x^T - x^S}, \tag{10}$$

або за формулою (11), якщо $S = T$

$$\lambda = \frac{3 \cdot x^S \circ x^S + a}{2 \cdot y^S}, \ \lambda = \frac{3 \cdot x^S \circ x^S + a}{2 \cdot y^S}, \tag{11}$$

де a – коефіцієнт ЕК.

Виконання умови гладкості

$$4 \cdot a \circ a \circ a + 27 \cdot b \circ b \neq (0, 0, ...) \tag{12}$$

забезпечує утворення групи точками ЕК.

В криптографії застосовуються гладкі ЕК з великим простим порядком групи точок. Порядок СВП дорівнює p^n, отже оцінку порядка групи точок ЕК над СВП $\# E(p)$ за теоремою Хассе [2] можна виразити наступним співвідношенням

$$p^n + 1 - 2 \cdot \sqrt{p^n} \leq \# E(p) \leq p^n + 1 + 2 \cdot \sqrt{p^n}. \tag{13}$$

Згідно з нижньою границею співвідношення (13), для досягнення порядку групи точок ЕК величиною, наприклад, 178 біт, необхідно використовувати просте число p величиною 90 біт за довжини вектора $n = 2$.

2 ПРОТОКОЛ СЛІПОГО ПІДПИСУ НА ОСНОВІ ГОСТ Р 34.10-2001

Розглянемо наступний протокол сліпого ЕЦП, запропонований в [3], який базується на стандарті ГОСТ Р 34.10-2001.

В схемі приймають участь дві сторони: підписувач А та абонент Б. Абонент Б виступає в якості емітента документа m, який підписувач А має підписати наосліп. Валідатором може виступити будь-хто з них або третя особа. Перевірка підпису відбувається за допомогою відкритого ключа підписувача А.

Загальні параметри: просте поле $GF(p)$, ЕК над цим полем з групою точок простого порядку q, базова точка P, хеш-функція $H()$.

Протокол складається з трьох етапів – генерація ключів, постановка підпису, перевірка підпису.

Під час генерації ключів секретний ключ d обирається випадково з діапазону $1 < d < q$. Відкритий ключ Q отримується з нього за формулою

$$Q = d \cdot P. \tag{14}$$

Етап постановки підпису починає підписувач А, обираючи одноразовий ключ k з діапазону $1 < k < q$ та обчислюючи точку E за формулою

$$E = k \cdot P = (x^E, y^E). \tag{15}$$

Підписувач А відправляє точку E абоненту Б.

Абонент Б формує хеш-образ повідомлення за співвідношенням

$$h = H(m). \tag{16}$$

Після цього він випадково обирає маскуючі параметри α та β з діапазону $1 < \alpha, \beta < q$ і обчислює точку C за формулою

$$C = \alpha \cdot E + \beta \cdot P = (x^C, y^C). \tag{17}$$

Абонент Б обчислює величини r та r' за формулами

$$r = x^C \bmod q, \tag{18}$$

$$r' = x^E \bmod q. \tag{19}$$

Ці величини використовуються в формулі засліплення хеш-образу повідомлення

$$h' = \frac{r'}{r} \cdot h \cdot \alpha \bmod q. \tag{20}$$

Абонент Б пересилає засліплений хеш-образ повідомлення h' підписувачу А.

Підписувач А ставить під ним засліплений підпис s' за допомогою власного секретного ключа d

$$s' = (d \cdot r' + k \cdot h') \bmod q, \tag{21}$$

та пересилає отримане значення абоненту Б.

Абонент Б має можливість перевірити справжність засліпленого підпису s' за допомогою співвідношення (22), використовуючи відкритий ключ Q підписувача А

$$s' \cdot P = r' \cdot Q + h' \cdot E. \tag{22}$$

Якщо засліплений підпис проходить перевірку, абонент Б формує з нього остаточний підпис

$$s = (s' \cdot \frac{r}{r'} + \beta \cdot h) \bmod q. \tag{23}$$

Сліпим підписом під документом m вважається пара значень $< r, s >$.

Валідатор при перевірці підпису $\{m, < r, s >\}$ обчислює точку R, використовуючи відкритий ключ Q підписувача А

$$R = \frac{s}{h} \cdot P - \frac{r}{h} \cdot Q = (x^R, y^R). \tag{24}$$

Підпис вважається справжнім, якщо виконується співвідношення

$$r = x^R \bmod q. \tag{25}$$

Автором було доведено в [4], що наведений протокол є захищеним за критерієм анонімності, тому він підходить для модифікації.

3 ПРОТОКОЛ СЛІПОГО ПІДПИСУ НА ЕК НАД СВП

Автором пропонується протокол сліпого підпису, який базується на вищенаведеному, однак використовує математичний апарат ЕК над СВП.

В схемі приймають участь дві сторони: підписувач А та абонент Б. Абонент Б виступає в якості емітента документа m, який підписувач А має підписати наосліп. Валідатором може виступити будь-хто з них або третя особа. Перевірка підпису відбувається за допомогою відкритого ключа підписувача А.

Загальні параметри: скінчене векторне поле з довжиною вектора n – розширення простого поля $GF(p)$, ЕК над цим полем з групою точок простого порядку q, базова точка P, хеш-функція $H()$.

Протокол складається з трьох етапів – генерація ключів, постановка підпису, перевірка підпису.

Під час генерації ключів секретний ключ d обирається випадково з діапазону $1 < d < q$. Відкритий ключ Q отримується з нього за формулою

$$Q = d \cdot P. \tag{26}$$

Оскільки ЕК задана над СВП, то при обчисленні суми двох точок в цій та подальших формулах використовуються співвідношення (8–11).

Етап постановки підпису починає підписувач А, обираючи одноразовий ключ k з діапазону $1 < k < q$, обчислюючи точку E за формулою

$$E = k \cdot P = (x^E, y^E) \tag{27}$$

та відправляючи цю точку абоненту Б.

Абонент Б формує хеш-образ повідомлення за співвідношенням

$$h = H(m). \tag{28}$$

Після цього він випадково обирає маскуючі параметри α та β з діапазону $1 < \alpha, \beta < q$ і обчислює точку C за формулою

$$C = \alpha \cdot E + \beta \cdot P = (x^C, y^C). \tag{29}$$

Абонент Б обчислює величини r та r' за формулами

$$r = \sum_{i=1}^{n} x_i^C \bmod q, \quad (30)$$

$$r' = \sum_{i=1}^{n} x_i^E \bmod q, \quad (31)$$

де $x^C = (x_1^C, x_2^C, ..., x_n^C)$, $x^E = (x_1^E, x_2^E, ..., x_n^E)$.

Абонент Б засліплює хеш-образ повідомлення за співвідношенням

$$h' = \frac{r'}{r} \cdot h \cdot \alpha \bmod q \quad (32)$$

і пересилає засліплений хеш-образ повідомлення h' підписувачу А.

Підписувач А формує засліплений підпис s' за допомогою власного секретного ключа d

$$s' = (d \cdot r' + k \cdot h') \bmod q, \quad (33)$$

та пересилає отримане значення абоненту Б.

Абонент Б має можливість перевірити справжність засліпленого підпису s' за допомогою співвідношення (34), використовуючи відкритий ключ Q підписувача А

$$s' \cdot P = r' \cdot Q + h' \cdot E. \quad (34)$$

Якщо засліплений підпис проходить перевірку, абонент Б формує з нього остаточний підпис

$$s = (s' \cdot \frac{r}{r'} + \beta \cdot h) \bmod q. \quad (35)$$

Сліпим підписом під документом m вважається пара значень $< r, s >$.

Валідатор при перевірці підпису $\{m, < r, s >\}$ обчислює точку R, використовуючи відкритий ключ Q підписувача А

$$R = \frac{s}{h} \cdot P - \frac{r}{h} \cdot Q = (x^R, y^R). \quad (36)$$

Підпис вважається справжнім, якщо виконується співвідношення

$$r = \sum_{i=1}^{n} x_i^R \bmod t. \quad (37)$$

де $x^R = (x_1^R, x_2^R, ..., x_n^R)$.

4 ОБЧИСЛЮВАЛЬНИЙ ПРИКЛАД ПРОТОКОЛУ СЛІПОГО ПІДПИСУ НА ЕК НАД СВП

Побудуємо СВП на основі простого поля $GF(11)$ з довжиною вектора $n = 2$. Правило множення задамо за табл. 1. З огляду на систему (5) значення розтягуючого коефіцієнта τ необхідно обирати з набору чисел $\{2, 6, 7, 8, 10\}$, які є квадратичними незалишками за модулем 11. Оберемо $\tau = 7$.

Розглянемо ЕК з коефіцієнтами $a = (1;3)$, $b = (5;6)$. Перевіримо умову гладкості (12) $4 \cdot (1;3) \circ (1;3) \circ (1;3) + 27 \cdot (5;6) \circ (5;6) = (0;3) \neq (0,0)$.

Базова точка $P = ((3;8),(4;9))$ має простий порядок $t = 113$.

Згенеруємо ключі підписувача А. Оберемо секретний ключ $d = 56$ та отримаємо за формулою (26) відкритий ключ $Q = 56 \cdot P = ((9;3),(9;9))$.

Підписувач А обирає одноразовий ключ $k = 28$ та обчислює за формулою (27) точку $E = 28 \cdot P = ((7;4),(0;3))$.

Абонент Б емітує документ з хеш-образом $h = 100$, обирає маскуючі параметри $\alpha = 44$ та $\beta = 75$, обчислює за формулою (29) точку $C = 44 \cdot E + 75 \cdot P = ((8;5),(10;0))$.

Після цього абонент Б обчислює за формулами (30–31) $r = x_1^C + x_2^C = 8 + 5 = 13$ та $r' = x_1^E + x_2^E = 7 + 4 = 11$ відповідно.

Абонент Б за формулою (32) засліплює повідомлення $h' = \frac{11}{13} \cdot 100 \cdot 44 \bmod 113 = 81$ та пересилає отримане значення підписувачеві А.

Підписувач А обчислює за формулою (33) засліплений підпис для отриманого значення $s' = (11 \cdot 56 + 28 \cdot 81) \bmod 113 = 59$ та відправляє його абонентові Б.

Абонент Б перевіряє справжність підпису за співвідношенням (34): в лівій частині співвідношення він отримує $59 \cdot P = ((5;2),(2;5))$, а в правій $11 \cdot Q + 81 \cdot E = ((5;2),(2;5))$. Оскільки значення в правій та лівій частинах перевірочного співвідношення збігаються, засліплений підпис вважається справжнім, і абонент Б обчислює за формулою (35) остаточний підпис $s = (59 \cdot \frac{13}{11} + 75 \cdot 100) \bmod 113 = 9$.

В результаті, під документом з хеш-образом $h = 100$ сформовано наосліп підпис $< r, s > = < 13, 9 >$.

Виконаємо перевірку сформованого підпису. За формулою (36) обчислимо точку $R = \frac{9}{100} \cdot P - \frac{13}{100} \cdot Q = ((8;5),(10;0))$. В правій частині перевірочного співвідношення (37) отримаємо $x_1^R + x_2^R = 8 + 5 = 13$. Ця величина збігається з $r = 13$, відповідно, підпис вважається справжнім.

Варто відзначити, що використання СВП в схемі сліпого ЕЦП не впливає на розмір підпису, зокрема, не призводить до його збільшення. Також важливо, що в процесі постановки підпису підписувач А не може дізнатися ні оригінального хеш-образу документу h, ні остаточного підпису $< r, s >$ під ним.

5 ПЕРЕВІРКА ЗАХИЩЕНОСТІ ПРОТОКОЛУ ЗА КРИТЕРІЄМ АНОНІМНОСТІ

Для схем сліпого підпису, на відміну від інших різновидів ЕЦП, актуальною є атака порушення анонімності. Спроба атаки може бути здійснена підписувачем за умови, що він зберігатиме всі відомі йому параметри схеми сліпого підпису разом із ідентифікатором емітента для кожної сесії постановки підпису. Накопичена база даних може бути використана в атаці, яка полягає у спробі визначення автора відомого документа m із підписом $< r, s >$, що проходить перевірку за допомогою відкритого ключа підписувача Q.

В запропонованому протоколі атака порушення анонімності може бути здійснена наступним чином. Підписувач А для кожного рядка своєї бази даних має обчислити ймовірні засліплюючи параметри α' та β' за формулами (38, 39)

$$\alpha' = \frac{r \cdot h'}{h \cdot r'} \bmod t, \tag{38}$$

$$\beta' = \frac{s - s' \cdot \frac{r}{r'}}{h} \bmod t, \tag{39}$$

За допомогою обчислених параметрів підписувач А для кожного рядка бази даних обчислює точку R' за формулою (40)

$$R' = \alpha' \cdot E + \beta' \cdot P = (x^{R'}, y^{R'}). \tag{40}$$

Рядок бази даних, для якого виконається співвідношення (41) має вказати на емітента повідомлення

$$r = \sum_{i=1}^{n} x_i^{R'} \bmod t. \tag{41}$$

Як доведено автором в [4], точка R' не залежить від параметрів h', r', s' і завжди збігається з перевірочною точкою R (див. співвідношення (36)), що не дає підписувачеві можливості визначити емітента.

$$R' = \alpha' \cdot E + \beta' \cdot P = \frac{r \cdot h'}{h \cdot r'} \cdot E + \frac{s - s' \cdot \frac{r}{r'}}{h} \cdot P =$$

$$= \frac{r}{h \cdot r'} \cdot \left(s' \cdot P - r' \cdot Q \right) + \frac{s}{h} \cdot P - \frac{s' \cdot r}{h \cdot r'} \cdot P = \frac{s}{h} \cdot P - \frac{r}{h} \cdot Q = R.$$

Таким чином, розглянутий протокол вважається захищеним за критерієм анонімності.

ВИСНОВКИ

В статті розглядається протокол сліпого електронного підпису на основі стандарту ГОСТ Р 34.10-2001 з використанням математичного апарату еліптичних кривих над скінченим векторним полем. Показано, що зміна математичного апарату не впливає на захищеність схеми сліпого підпису за критерієм анонімності.

В подальшому автором планується оцінка виграшу в швидкодії та ресурсомісткості при використанні математичного апарату ЕК над СВП в схемах ЕЦП з рекомендованими параметрами.

СПИСОК ЛІТЕРАТУРИ

1. *Молдовян, Н. А.* Теоретический минимум и алгоритмы цифровой подписи / Н. А. Молдовян. – С. Пб. : БХВ-Петербург, 2010. – 304 с.
2. Алгоритмические основы эллиптической криптографии / [Болотов А. А., Гашков С. Б., Фролов А. Б., Часовских А. А.]. – М. : Мэи, 2000. – 100 с.
3. *Костин, А. А.* О реализации протоколов слепой подписи и коллективной подписи на основе стандартов цифровой подписи / Костин А. А., Молдовян Н. А.,Фаль А. М. // Материалы VI Санкт-Петербургской межрегиональной конференции «Информационная безопасность России (ИБРР-2009). Санкт-Петербург, 28 30 октября 2009. – С. Пб. : СПОИСУ, 2009. – С. 111.
4. *Нікуліщев, Г. І.* Анонімність як критерій оцінки захищеності протоколів сліпого електронного цифрового підпису / Г. І. Нікуліщев, Г. Л. Козина // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2012. – № 2.– С. 52–59.

Стаття надійшла до редакції 19.09.2013.

Никулищев Г. И.
Старший преподаватель, Запорожский национальный технический университет, Украина

ПРОТОКОЛ СЛЕПОЙ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ НАД КОНЕЧНЫМ ВЕКТОРНЫМ ПОЛЕМ

В данной статье предлагается реализация протокола слепой электронной цифровой подписи, представляющего собой модификацию стандарта ГОСТ Р 34.10-2001 на эллиптических кривых над конечным векторным полем. Анализируется защищенность предлагаемого протокола по критерию анонимности.

Ключевые слова: слепая электронная цифровая подпись, конечное векторное поле, эллиптическая кривая.

Nikulishchev H. I.
Senior tutor, Zaporizhzhia national technical university, Ukraine

BLIND DIGITAL SIGNATURE PROTOCOL ON ELLIPTIC CURVES OVER VECTOR FINITE FIELD

Digital signature schemes can fulfill an actual task of ensuring fairness and transparency of electronic election. However, existing standards and protocols need modification into blind signature and additional security check by the anonymity criterion. The author examines blind signature protocol provided by Russian scientists. It is proposed to improve scheme's efficiency by changing inner mathematics. Elliptic curves over vector finite field enable parallel processing in group operation and reduce integer range. These advantages are illustrated by computational example. Also, improved protocol investigation by the anonymity criterion is provided in the article. The author proves that mathematics change do not affect protocol security.

Keywords: blind digital signature, vector finite field, elliptic curve.

REFERENCES

1. Moldovyan N. A. Teoreticheskij minimum i algoritmy' cifrovoj podpisi. Sankt-Peterburg, BXV-Peterburg, 2010, 304 p.
2. Bolotov A. A., Gashkov S. B., Frolov A. B., Chasovskix A. A. Algoritmicheskie osnovy' e'llipticheskoj kriptografii. Moscow, Me'i, 2000, 100 p.
3. Kostin A. A., Moldovyan N. A., Fal' A. M. O realizacii protokolov slepoj podpisi i kollektivnoj podpisi na osnove standartov cifrovoj podpisi. *Materialy' VI Sankt-Peterburgskoj mezhregional'noj konferencii «Informacionnaya bezopasnost' Rossii (IBRR-2009)». Sankt-Peterburg, 28–30 oktyabrya 2009,* Sankt-Petersburg, SPOISU, 2009, pp. 111.
4. Nikulishchev H. I., Kozina H. L. Anonimnist yak kryterii otsinky zakhyshchenosti protokoliv slipoho elektronnoho tsyfrovoho pidpysu. *Pravove, normatyvne ta metrolohichne zabezpechennia systemy zakhystu informatsii v Ukraini*, 2012, No. 2, pp. 52–59.