УДК 004.056.55

МАТЕМАТИЧНА МОДЕЛЬ ПРОТОКОЛУ СЛІПОГО ЕЛЕКТРОННОГО ПІДПИСУ НА ЕЛІПТИЧНИХ КРИВИХ

М.В. ЄСІНА

У роботі розглядається математична модель протоколу сліпого електронного підпису на основі алгоритму ECDSA та алгоритмі, який описано у ДСТУ 4145-2002. Проводиться перевірка захищеності протоколу на основі цих алгоритмів за критерієм анонімності.

Ключові слова: анонімність, електронний підпис, сліпий підпис.

ВСТУП

Сліпий підпис знаходить широке застосування в протоколах електронного голосування та електронних грошей. В його основу, як правило, покладається електронний підпис (ЕП). В ході застосування сліпого підпису надається послуга анонімності (невідстежуваності), яка є обов'язковою в системах таємного електронного голосування та системах електронних грошей.

У типовій схемі сліпого підпису приймають участь, як правило, три сторони [5] – емітент документа, підписувач та перевірник (валідатор). Емітент створює документ, який підписувач має підписати анонімно. Тобто, підписувач не повинен знати вміст документа та вигляд остаточного підпису. Для цього емітент маскує документ за допомогою певного криптографічного перетворення. Підписувач підписує замаскований документ, а емітент на основі його підпису формує остаточний ЕП під документом у відкритому вигляді. Перевірник перевіряє правильність підпису за допомогою відкритого ключа емітента.

У [5, 6] запропоновані механізми (протоколи) сліпого ЕП, які ґрунтуються на алгоритмах ГОСТ 34.10-2001, Шнора та Ель Гамаля. Але сьогодні в Україні дозволеними чи такими, що рекомендуються до застосування, є алгоритми ЕП, що визначені в ДСТУ ISO/IEC 14888-3:2014 та ДСТУ 4145-2002. Тому важливою є задача розробки та детального дослідження вказаних алгоритмів ЕП з точки зору їх застосування в механізмах сліпого підпису.

Метою цієї статті є розробка пропозицій з побудови та дослідження механізму сліпого підпису на основі використання ЕП, що визначені в ДСТУ ISO/IEC 14888-3:2014 (ECDSA) та ДСТУ 4145-2002.

1. ЗАГАЛЬНИЙ ОПИС ПРОТОКОЛУ СЛІПОГО ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ НА ЕЛІПТИЧНИХ КРИВИХ

У схемі приймають участь дві сторони: А – підписувач, В – абонент (емітент документа / повідомлення m). Перевіряючим (валідатором) може виступати будь-хто з них, або довірена третя особа [5].

Загальні параметри:

- просте поле $GF(p)$;
- ЕК над цим полем;
- n – порядок базової точки;
- G – базова точка;
- функція гешування $H()$.

Протокол складається з трьох етапів:

1) генерація ключів,
2) постановка підпису,
3) перевірка підпису.

Під час генерації ключів секретний ключ d обирається випадково з діапазону $1 < d < (n-1)$. З нього формується відкритий ключ Q за відповідною формулою.

Етап постановки підпису починає підписувач А. Він обирає k (в деяких стандартах позначається як e) – випадкове число із діапазону $1 < k < (n-1)$ та обчислює точку E.

Підписувач А відправляє точку E абоненту В.

Абонент В формує геш-образ повідомлення h.

Після цього В обирає маскуючий параметр α, $1 < \alpha < n-1$.

Далі він обчислює точку C.

Абонент В обчислює величини r та r'.

Ці величини використовуються для засліплення геш-образу повідомлення h'.

Абонент В пересилає h' підписувачу А.

Підписувач А ставить під засліпленим геш-образом повідомлення h' засліплений підпис s' за допомогою свого власного секретного ключа d та пересилає отримане значення абоненту В.

Абонент В має можливість перевірити справжність засліпленого підпису s' за допомогою звичайної перевірки підпису, що описана у відповідному стандарті, використовуючи відкритий ключ Q підписувача А.

Якщо s' проходить перевірку, абонент В формує з нього остаточний підпис.

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

Перевіряючий (валідатор) під час перевірки підпису $\{m,<r,s>\}$ обчислює точку R, для чого використовує звичайну перевірку підпису, що описана у відповідному стандарті, використовуючи відкритий ключ Q підписувача А.

Підпис вважається справжнім, якщо виконується таке співвідношення: $r = x_R \bmod n$.

2. 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 [5].

У запропонованому протоколі атака порушення анонімності може бути здійснена наступним чином. Підписувач А для кожного рядка своєї бази даних повинен обчислити ймовірний засліплюючий параметр α' [6].

За допомогою обчислених параметрів підписувач А для кожного рядка бази даних обчислює точку R'.

Рядок бази даних, для якого виконується наступне співвідношення, має вказати на емітента повідомлення:

$$r = x_{R'} \bmod n .$$

Доведемо, що точка R' завжди збігається з перевірною точкою R і не залежить від параметрів h',r',s' і, отже, не дає можливості визначити автора документа m. Для доведення цього твердження використовується рівність R' стандартній перевірці цифрового підпису у відповідному стандарті.

Розглянуті протоколи вважаються захищеними за критерієм анонімності, тому що неможливо визначити автора документа m.

3. ПРОТОКОЛ СЛІПОГО ПІДПИСУ НА ОСНОВІ ДСТУ ISO/IEC 14888-3:2014 (ECDSA)

У таблицях 1 та 2 наведені параметри протоколу сліпого підпису на основі алгоритму цифрового підпису ECDSA [1].

Доведемо, що наведені формули відповідають дійсності: абонент В формує із сліпого ЕП остаточний підпис:

$$s = \frac{s'\cdot(r/r')}{\alpha} \bmod n . \qquad (1)$$

Перевіряючий (валідатор) під час перевірки підпису $\{m,<r,s>\}$ обчислює точку R, для чого використовує відкритий ключ Q підписувача А:

$$R = (\frac{h}{s}\cdot G + \frac{r}{s}\cdot Q) \bmod n = (x_R, y_R) . \qquad (2)$$

Покажемо, що математичний вираз остаточного підпису s проходить перевірку валідатора:

$$R = (\frac{h}{s}\cdot G + \frac{r}{s}\cdot Q) \bmod n = \frac{dr+h}{s}\cdot G \bmod n =$$
$$= \frac{k\alpha G(dr+h)}{(dr'+h')\cdot r/r'} \bmod n = \frac{k\alpha G(dr+h)}{(dr'+\frac{r'}{r}\cdot h)\cdot r/r'} \bmod n = \qquad (3)$$
$$= \frac{k\alpha G(dr+h)}{dr+h} \bmod n = k\alpha G \bmod n =$$
$$= \alpha E \bmod n = (x_R, y_R) = C = (x_C, y_C).$$

Таблиця 1

Вирази для сліпого та остаточного підпису, та їх перевірки

Параметри	ECDSA
Засліплений підпис	$s' = \frac{d\cdot r' + h'}{k} \bmod n$
Перевірка засліпленого підпису	$R' = (\frac{h'}{s'}\cdot G + \frac{r'}{s'}\cdot Q) \bmod n$
Остаточний підпис	$s = \frac{s'\cdot(r/r')}{\alpha} \bmod n$
Перевірка остаточного підпису	$R = (\frac{h}{s}\cdot G + \frac{r}{s}\cdot Q) \bmod n = (x_R, y_R)$, $r = x_R \bmod n$

Таблиця 2

Параметри протоколу сліпого ЕП та перевірки захищеності протоколу за критерієм анонімності

Параметри	ECDSA
Відкритий ключ	$Q = d\cdot G \bmod n$
Точка E	$E = k\cdot G \bmod n = (x_E, y_E)$
Геш-значення	$h = H(m)$
Точка C	$C = \alpha\cdot E \bmod n = (x_C, y_C)$
Величини r та r'	$r = x_C \bmod n$, $r' = x_E \bmod n$
Засліплений геш-образ	$h' = (\frac{r'}{r}\cdot h) \bmod n$
Параметр для перевірки на анонімність	$\alpha' = \frac{s'\cdot(r/r')}{s} \bmod n$
Перевірка на анонімність	$R' = \alpha'\cdot E \bmod n = (x_{R'}, y_{R'})$ => $R' = (\frac{r}{s}\cdot Q + \frac{h}{s}\cdot G) \bmod n$, $r = x_{R'} \bmod n$

У запропонованому протоколі атака порушення анонімності може бути здійснена наступним чином. Підписувач А для кожного рядка своєї бази даних повинен обчислити ймовірний засліплюючий параметр α':

$$\alpha' = \frac{s'\cdot(r/r')}{s} \bmod n . \qquad (4)$$

За допомогою обчислених параметрів підписувач А для кожного рядка бази даних обчислює точку R' за допомогою такої формули:

$$R' = \alpha'\cdot E \bmod n = (x_{R'}, y_{R'}) . \qquad (5)$$

Доведемо, що точка R' завжди збігається з перевірочною точкою R і не залежить від параметрів h',r',s' і, отже, не дає можливості визначити автора документа m. Для доведення цього твердження використовуватимемо рівність R' стандартній перевірці цифрового підпису ECDSA:

$$R' = \alpha'\cdot E \bmod n = \frac{s'\cdot(r/r')}{s}\cdot E \bmod n =$$
$$= \frac{\frac{dr'+h'}{k}\cdot\frac{r}{r'}}{s}\cdot E \bmod n = \frac{\frac{dr'+\frac{r'}{r}\cdot h}{k}\cdot\frac{r}{r'}}{s}\cdot E \bmod n = \qquad (6)$$

$$= \frac{\frac{dr+h}{k}}{s} \cdot E \bmod n = \frac{dr+h}{ks} \cdot kG \bmod n = \\ = (\frac{dr}{s} \cdot G + \frac{h}{s} \cdot G) \bmod n = (\frac{r}{s} \cdot Q + \frac{h}{s} \cdot G) \bmod n. \quad (6)$$

Отже, розглянутий протокол вважається захищеним за критерієм анонімності, тому що неможливо визначити автора документа m.

4. ПРОТОКОЛ СЛІПОГО ПІДПИСУ НА ОСНОВІ ДСТУ 4145-2002

У таблицях 3 та 4 наведено параметри протоколу сліпого підпису на основі алгоритму цифрового підпису ДСТУ [3].

Таблиця 3

Вирази для сліпого та остаточного підпису, та їх перевірки

Параметри	ДСТУ
Засліплений підпис	$s' = (e + dr') \bmod n$
Перевірка засліпленого підпису	$R' = (s' \cdot G + r' \cdot Q) \bmod n$
Остаточний підпис	$s = s' \cdot \alpha \bmod n$
Перевірка остаточного підпису	$R = (s \cdot G + r \cdot Q) \bmod n = (x_R, y_R)$, $r = x_R \bmod n$

Таблиця 4

Параметри протоколу сліпого ЕП та перевірки захищеності протоколу за критерієм анонімності

Параметри	ДСТУ
Відкритий ключ	$Q = -d \cdot G \bmod n$
Точка E	$E = k \cdot G \bmod n = (x_E, y_E)$
Геш-значення	$h = H(m)$
Точка C	$C = \alpha \cdot E \bmod n = (x_C, y_C)$
Величини r та r'	$r = h \cdot x_C \bmod n$, $r' = h' \cdot x_E \bmod n$
Засліплений геш-образ	$h' = \frac{x_C \cdot h}{x_E \cdot \alpha} \bmod n$
Параметр для перевірки на анонімність	$\alpha' = \frac{s}{s'} \bmod n$, $\alpha' = \frac{x_C \cdot h}{x_E \cdot h'} \bmod n = \frac{r}{r'} \bmod n$
Перевірка на анонімність	$R' = \alpha' \cdot E \bmod n = (x_{R'}, y_{R'}) \Rightarrow R' = (s \cdot G + r \cdot Q) \bmod n$, $r = x_{R'} \bmod n$

Доведемо, що наведені формули відповідають дійсності: абонент В формує із сліпого ЕП остаточний підпис:

$$s = s' \cdot \alpha \bmod n. \quad (7)$$

Перевіряючий (валідатор) під час перевірки підпису $\{m, <r, s>\}$ обчислює точку R, для чого використовує відкритий ключ Q підписувача А:

$$R = (s \cdot G + r \cdot Q) \bmod n = (x_R, y_R). \quad (8)$$

Покажемо, що математичний вираз остаточного підпису s проходить перевірку валідатора:

$$R = (s \cdot G + r \cdot Q) \bmod n = \\ = ((e + dr')\alpha G + rQ) \bmod n = \\ = (\alpha e G + \alpha r' dG + rQ) \bmod n = \\ = (\alpha E + \alpha h' x_E dG + rQ) \bmod n = \\ = (\alpha E + rQ + \alpha Q x_E \frac{x_C \cdot h}{x_E \cdot \alpha}) \bmod n = \\ = (\alpha E + rQ + x_C h Q) \bmod n = \\ = (\alpha E - rdG + rQ) \bmod n = \\ = (\alpha E - rdG + rdG) \bmod n = \\ = \alpha E \bmod n = (x_R, y_R) = C = (x_C, y_C). \quad (9)$$

У запропонованому протоколі атака порушення анонімності може бути здійснена наступним чином. Підписувач А для кожного рядка своєї бази даних повинен обчислити ймовірний засліплюючий параметр α':

– виходячи з формули остаточного підпису

$$\alpha' = \frac{s}{s'} \bmod n. \quad (10)$$

– виходячи з формули засліпленого геш-значення

$$\alpha' = \frac{x_C \cdot h}{x_E \cdot h'} \bmod n = \frac{r}{r'} \bmod n. \quad (11)$$

За допомогою обчислених параметрів підписувач А для кожного рядка бази даних обчислює точку R' за допомогою такої формули:

$$R' = \alpha' \cdot E \bmod n = (x_{R'}, y_{R'}). \quad (12)$$

Доведемо, що точка R' завжди збігається з перевірною точкою R і не залежить від параметрів h', r', s' і, отже, не дає можливості визначити автора документа m. Для доведення цього твердження використовуватимемо рівність R' стандартній перевірці цифрового підпису ДСТУ:

$$R' = \alpha' \cdot E \bmod n = eG \frac{r}{r'} \bmod n = \\ = G \frac{r}{r'} (s' - dr') \bmod n = \\ = (G \frac{r}{r'} s' - G \frac{r}{r'} s \cdot dr') \bmod n = \\ = (G \frac{r}{r'} s' - rdG) \bmod n = \\ = (\alpha s' G - rdG) \bmod n = (s \cdot G + r \cdot Q) \bmod n. \quad (13)$$

Отже, розглянутий протокол вважається захищеним за критерієм анонімності, тому що неможливо визначити автора документа m.

5. АТАКИ НА ПРОТОКОЛ СЛІПОГО ПІДПИСУ

На сліпий підпис існують різноманітні атаки. Ці атаки такі ж самі як і атаки на звичайні ЕП. Це досягається за допомогою того, що у нашому випадку протокол сліпого підпису побудовано на основі відповідних стандартів алгоритмів ЕП. Алгоритм формування сліпого підпису співпадає зі звичайним алгоритмом побудови ЕП відповідного стандарту, а формування остаточного

підпису у протоколі використовує раніше сформований сліпий підпис, який множиться або ділиться на випадкове число. Жодних інших операцій не використовується.

Зважаючи на все вищевказане, можна стверджувати, що сліпому та остаточному підпису у протоколі сліпого підпису загрожують аналогічні атаки.

5.1. Атака «повне розкриття» на основі підписаних даних

Стійкість двох розглянутих вище алгоритмів ЕП заснована на складності розв'язання дискретного логарифму в групі точок еліптичної кривої. Для знаходження секретного ключа необхідно розв'язати відносно d рівняння на основі обчислення відкритого ключа Q, що індивідуальні для кожного з розглянутих алгоритмів [4].

Як було вказано вище, маємо однакові атаки на стандартні алгоритми ЕП та на протоколи сліпого підпису, на основі цих алгоритмів. Отже, можна розглядати атаку «повне розкриття» для протоколів сліпого підпису таким же чином, як і для стандартних алгоритмів ЕП.

Розглянемо можливість знаходження d на основі атаки при відомих підписаних (перехоплених) повідомленнях. Нехай перехоплено і підписано повідомлення [3].

Сліпий підпис для ECDSA має такий вигляд

$$s' = \frac{d \cdot r' + h'}{k} \bmod n \qquad (14)$$

тобто, відносно d, отримаємо таке:

$$\begin{cases} d = \dfrac{k_1 s'_1 - h'_1}{r'_1} \bmod n \\ \ldots \\ d = \dfrac{k_i s'_i - h'_i}{r'_i} \bmod n \end{cases}. \qquad (15)$$

Сліпий підпис для ДСТУ 4145-2002 має такий вигляд

$$s' = (e + dr') \bmod n \qquad (16)$$

тобто, відносно d, отримаємо:

$$\begin{cases} d = \dfrac{s'_1 - e'_1}{r'_1} \bmod n \\ \ldots \\ d = \dfrac{s'_i - e'_i}{r'_i} \bmod n \end{cases}. \qquad (17)$$

Отже, у випадку сліпого підпису також маємо систему рівнянь порядку i рівнянь з $i+1$ невідомими. Тобто не маємо жодної різниці зі стандартним алгоритмом.

Тепер розглянемо ситуацію з остаточним підписом у протоколі сліпого підпису.

У ході формування остаточного сліпого підпису використовується раніше сформований засліплений підпис, який лише множиться або ділиться на визначене випадкове число. Жодних інших дій при формуванні остаточного підпису не проводиться.

Остаточний підпис у ході використання ECDSA має такий вигляд

$$s = \frac{s' \cdot (r / r')}{\alpha} \bmod n, \qquad (18)$$

де α – випадкове число із визначеного діапазону, $\frac{r}{r'}$ – відношення двох координат (також просто число).

Розпишемо s повністю та одержимо відносно d необхідний вираз

$$s = \frac{(e + dr') \cdot \frac{r}{r'}}{\alpha} \bmod n = \frac{e \cdot \frac{r}{r'} + dr}{\alpha} \bmod n. \qquad (19)$$

$$\begin{cases} d = \dfrac{s_1 \alpha - e_1 \frac{r_1}{r'_1}}{r_1} \bmod n \\ \ldots \\ d = \dfrac{s_i \alpha - e_i \frac{r_i}{r'_i}}{r_i} \bmod n \end{cases}. \qquad (20)$$

Остаточний підпис у ході використання ДСТУ 4145-2002 має такий вигляд

$$s = s' \cdot \alpha \bmod n, \qquad (21)$$

де α – випадкове число із визначеного діапазону.

Розпишемо s повністю та одержимо відносно d необхідний вираз

$$s = (e + dr')\alpha \bmod n = (e\alpha + dr'\alpha) d \bmod n \qquad (22)$$

$$\begin{cases} d = \dfrac{s_1 - e_1 \alpha}{r'_1 \alpha} \bmod n \\ \ldots \\ d = \dfrac{s_i - e_i \alpha}{r'_i \alpha} \bmod n \end{cases}. \qquad (23)$$

Як видно з наведених виразів для усіх розглянутих алгоритмів ЕП, сформований остаточний підпис у протоколі сліпого підпису має той самий вигляд, що і стандартний ЕП. Відмінність лише у наявності відповідних коефіцієнтів при основних значеннях. Але ці коефіцієнти – випадкові числа і жодним чином не впливають на стійкість до атаки.

Таким чином, для повного розкриття, тобто визначення секретного ключа d за i отриманим ЕП, необхідно розв'язувати систему i-го порядку з $i+1$ невідомими [4].

У разі, якщо повідомлення M є зашифрованим, невідомими є значення функцій гешування $h_1, h_2, \ldots, h_i$. Як результат одержимо систему рівнянь з $2i+1$ невідомими, тому шифрування підписаних повідомлень дозволяє істотно підвищити стійкість.

5.2. Аналіз захищеності ЕП від атак на реалізацію

Нехай розробник може закласти лазівку у програмну реалізацію вироблення підпису. Нижче наводяться теоретичні та експериментальні результати відносно захищеності сліпого підпису у протоколах сліпого ЕП на основі стан-

дартних алгоритмів ЕП від таких атак для двох розглянутих вище алгоритмів [4].

Для ECDSA порушнику відомо:

$$r'_1 = \pi(x_1, y_1) = x_1 \bmod n, \quad (24)$$

$$r'_2 = \pi(x_1, -y_1) = x_1 \bmod n. \quad (25)$$

Таким чином

$$r'_1 = r'_2 = x_1 \bmod n. \quad (26)$$

Для s'_1 та s'_2 маємо:

$$s'_1 = \frac{dr'_1 + h'_1}{k_1} \bmod n, \quad (27)$$

$$s'_2 = \frac{dr'_2 + h'_2}{k_1} \bmod n. \quad (28)$$

Оскільки $k_1 = k_2 = k$ та $r'_1 = r'_2 = x_1 \bmod n$, то

$$s'_1 = \frac{dr' + h'_1}{k_1} \bmod n, \quad (29)$$

$$s'_2 = \frac{dr' + h'_2}{k_1} \bmod n. \quad (30)$$

Розв'язавши відносно d та k маємо:

$$d = \frac{s'_1 h'_2 - s'_2 h'_2}{r'(s'_2 - s'_1)} \bmod n; \quad (31)$$

$$k = \frac{dr' + h'_1}{s'_1} \bmod n. \quad (32)$$

Для ДСТУ 4145-2002 пропонуємо:

$$k_1 = k_2 = k \in (1, n-1); \quad (33)$$

$$R_1 = R_2 = kG = (x_R, y_R) = R; \quad (34)$$

$$fk_1 = fk_2 = x_R = fk; \quad (35)$$

$$y_1 = h'_1 fk; \quad (36)$$

$$y_2 = h'_2 fk; \quad (37)$$

$$y_1 \Rightarrow r'_1; y_2 \Rightarrow r'_2; \quad (38)$$

Для s'_1 та s'_2 маємо:

$$s'_1 = (k + dr'_1) \bmod n; \quad (39)$$

$$s'_2 = (k + dr'_2) \bmod n. \quad (40)$$

Розв'язуючи (39) та (40) відносно (k,d) маємо:

$$d = \frac{s'_1 - s'_2}{r'_1 - r'_2} \bmod n, \quad (41)$$

$$k = (s'_1 - dr'_1) \bmod n. \quad (42)$$

Для протоколів сліпого підпису на основі алгоритмів ЕП ECDSA та ДСТУ 4145-2002 існують атаки на програмну реалізацію ЕП. Якщо зловмиснику вдасться змусити програму «вироблення підпису» двічі використати одне і те саме значення k для двох повідомлень, то він в реальному часі визначить особистий довгостроковий ключ d і зможе нав'язувати як хибні повідомлення, так і викривляти істинні.

Для захисту від такої атаки необхідно використовувати надійні засоби КЗІ типу ЕП у змісті наявності на них сертифікатів відповідності, експертних висновків та можливості безперервного контролю цілісності та справжності програми вироблення ЕП. Кращим способом забезпечення захисту від такої загрози є апаратна реалізація процедур вироблення та перевіряння ЕП [4].

5.3. Аналіз захищеності сліпого ЦП від атаки на анонімність

Як вказано вище, усі алгоритми проходять перевірку на анонімність і, навіть, якщо підписувач A зберігатиме усі параметри h', r', s', то в подальшому він не зможе встановити відповідність цих параметрів до емітента, для якого підпис було виконано. Але, якщо для алгоритму ECDSA це правильно повною мірою, то для інших є особливість – α' виражається двома виразами, які прийматимуть однакове значення лише для абонента B, що формував остаточний підпис за цими параметрами (ймовірність того, що буде ще один емітент, для якого два вирази α' матимуть однакове значення, дорівнює 2^{-n}). З цього випливає, що наведений механізм для EKGDSA, ECKCDSA та ДСТУ забезпечує сліпий підпис з відстежуваною анонімністю [2].

Змінити це можливо за допомогою апаратних чи апаратно-програмних засобів криптографічного захисту інформації (КЗІ). Використання таких засобів для сліпого підпису подібно використанню криптографічних модулів для генерації ключів користувачів у центрах сертифікації ключів (ЦСК). Користувач може згенерувати свій ключ на станції в самому центрі, але завдяки тому, що було використано сертифікований засіб КЗІ, користувач може бути впевнений в тому, що тільки він володіє ключем і у ЦСК не залишилися копії цього ключа.

Таким же чином можливо використання криптографічного модуля для сліпого підпису. Нехай буде мікромодуль D, в якому буде записана асиметрична пара ключів для виконання підпису та забезпечення конфіденційності при отриманні заслiпленого геш-образу. В такому випадку підписувач A – лише оператор криптомодуля D, який не має прямого доступу до ключів (або D може повністю заміщати A, тоді емітенту В надається доступ до роботи із засобом КЗІ). Виконуються такі операції:

1) абонент В направлено зашифровує h' на відкритому ключі криптомодуля D;

2) отримане $E_D(h')$ надсилається D (прямо чи за допомогою оператора A);

3) D розшифровує h' та створює s';

4) r' та s' відсилаються емітенту B, а h' вилучається з пам'яті D.

Через те, що h' обробляється лише у D і A немає можливості розшифрувати $E_D(h')$, підписувач не зможе здійснити атаку на анонімність, бо в нього не буде одного з параметрів.

Такий підхід може використовуватися при наданні послуг сліпого ЕП у хмарах. Також одним з прикладів використання сліпого підпису на основі засобів КЗІ є проведення виборів. Виборці заходять до кабінки, де стоїть автома-

тизована станція (АС), що оснащена криптографічним модулем; формують список голосів за кандидатів (повідомлення); виробляють підпис та надсилають його. За допомогою механізму сліпого підпису і використання запрограмованого на це засобу КЗІ, забезпечується анонімність голосування і підтверджується дійсність та цілісність кожного голосу.

ВИСНОВКИ

Розглянувши алгоритми ЕП, що базуються на стандартах ДСТУ ISO/IEC 14888-3:2014 (ECDSA) та ДСТУ 4145-2002 [1, 3], було побудовано на їх основі протокол сліпого електронного підпису. Дослідивши схеми даних сліпих електронних підписів, було визначено, що ці схеми стійкі за критерієм анонімності. Також дослідження цих схем показує, що співвідношення між маскуючими параметрами необхідно обирати таким чином, щоб за ними було неможливо вирахувати автора документу, що ставить підпис під документом [5, 6].

Перевагою запропонованого методу сліпого підпису над існуючими є те, що дії підписувача та валідатора такі самі, як описано у відповідних стандартах для звичайного підпису та перевірки в групі точок еліптичних кривих. Відмінність полягає лише в тому, що підписувач отримує геш-значення, а не знаходить його сам. Кроки, що відрізняють сліпий підпис від звичайного, виконуються емітентом. Така методика робить впровадження функціоналу сліпого підпису в існуючі інформаційно-телекомунікаційні системи таким, що майже не потребує додаткових зусиль. Необхідно лише реалізувати протокол для емітента, а підписувач та валідатор можуть використовувати вже існуючі засоби створення та перевірки ЕП.

Також даний метод має переваги під час розробки стандартів. Такий підхід дозволяє напряму посилатися на існуючі стандарти і не вступати з ними в протиріччя (перевірка підпису за одним стандартом, як для ЕП так і для сліпого підпису).

Через те, що алгоритми сліпого підпису у протоколі сліпого ЕП співпадають з алгоритмами ЕП відповідних стандартів, то алгоритми сліпого підпису є уразливими до тих самих атак, що і стандартні алгоритми ЕП. При формуванні остаточного підпису стандартний алгоритм ЕП також зберігається, тому що остаточний підпис формується зі сліпого, який множиться або ділиться на випадкове число, яке жодним чином не впливає на стійкість до атак.

В ході використання даного механізму ECDSA забезпечує повну анонімність, а ДСТУ 4145 – лише відстежувану. Для забезпечення повної анонімності необхідно використовувати засоби КЗІ. Іншим варіантом є переробка самого механізму, але це призведе до втрати усіх його переваг і може лише в подальшому слугувати альтернативою використанню апаратних криптографічних модулів.

Література

[1] Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms : ISO/IEC 14888-3 (Edition 2 (2006-11-15)) : 2006. – 68 p.

[2] Information technology – Security techniques – Blind digital signatures – Part 2: Discrete logarithm based mechanisms : ISO/IEC DIS 18370-2:2014(E):2015. – 70 p.

[3] Інформаційні технології – Криптографічний захист інформації – Цифровий підпис, що ґрунтується на еліптичних кривих – Формування та перевірка : ДСТУ 4145-2002. – К. : Держстандарт України, 2003. – 35 с. – (Національні стандарти України).

[4] *Горбенко І.Д., Горбенко Ю.І.* Прикладна криптологія. Теорія. Практика. Застосування: монографія. Харків: «Форт», 2012. – 870 с.

[5] *Нікуліщев Г. І.* Протокол сліпого електронного цифрового підпису на еліптичних кривих над скінченим векторним полем / Г. І. Нікуліщев // Радіоелектроніка, інформатика, управління. – 2013, № 2. – С. 71–76.

[6] *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. 59–65.

Надійшла до редколегії 24.11.2015

Єсіна Марина Віталіївна, аспірантка факультету комп'ютерних наук, кафедри безпеки інформаційних систем і технологій Харківського національного університету імені В.Н. Каразіна. Наукові інтереси: електронний підпис, методи багатофакторної автентифікації та їх застосування з метою захисту інформації.

УДК 004.056.55

Математическая модель протокола слепой электронной подписи на элиптических кривых / Есина М.В. // Прикладная радиоэлектроника: науч.-техн. журнал. – 2015. – Том 14. – № 4. – С. 300–305.

В работе рассматривается математическая модель протокола слепой электронной подписи на основе алгоритма ECDSA и алгоритма, который описан в ДСТУ 4145-2002. Проводится проверка защищенности протокола на основе этих алгоритмов по критерию анонимности.

Ключевые слова: анонимность, электронная подпись, слепая подпись.

Табл.: 4. Библиогр.: 6 назв.

UDC 004.056.55

Mathematical model of a protocol of blind electronic signature based on eliptic curves / M.V. Yesina // Applied Radio Electronics: Sci. Journ. — 2015. — Vol. 14. — № 4. — P. 300–305.

The paper deals with a mathematical model of a protocol of electronic signature based on the algorithm ECDSA and algorithm that is described in DSTU 4145-2002. Testing the protocol security based on these algorithms by the criterion of anonymity has been performed.

Keywords: anonymity, digital signature, blind signature.

Tab.: 4. Ref.: 6 items.