

МАТЕМАТИЧНА МОДЕЛЬ ПРОТОКОЛУ СЛІПОГО ЕЛЕКТРОННОГО ПІДПISY НА ОСНОВІ АЛГОРИТМІВ ECGDSA ТА ECKCDSA

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

На даний момент комітетом ISO/IEC JTC 1/SC 27 (одним з учасників якого є Україна) розробляється пакет стандартів стосовно електронних довірчих послуг. Сліпий підпис є однією з таких послуг і стосовно нього розробляється міжнародний стандарт ISO/IEC DIS 18370-2 [2], що буде регламентувати види сліпого підпису, їх використання та стандарти конкретних механізмів і протоколів сліпого підпису.

У типовій схемі сліпого підпису беруть участь, як правило, три сторони [4] – емітент документу, підписувач та перевірник (валідатор). Емітент створює документ, який підписувач має підписати анонімно. Особливість сліпого підпису полягає в тому, що підписувач не повинен знати вміст документа та вигляд остаточного підпису. Для цього емітент маскує документ за допомогою певного криптографічного перетворення (створює засліплений геш-образ повідомлення). 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 [4, 5] запропоновано механізми (протоколи) сліпого ЕП, які ґрунтуються на алгоритмах ГОСТ 34.10 - 2001, Шнора та Ель Гамала. Але нині в Україні дозволеними чи такими, що рекомендуються до застосування, є алгоритми ЕП, що визначені в ДСТУ ISO/IEC 14888-3:2014. Тому важливою є задача розробки та детального дослідження вказаних алгоритмів ЕП з точки зору їх застосування в механізмах сліпого підпису.

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

Загальний опис протоколу сліпого електронного цифрового підпису на еліптичних кривих

У схемі беруть участь дві сторони: А – підписувач, В – абонент (емітент документу/повідомлення m). Перевіряючим (валідатором) може виступати будь-хто з них, або довірена третя особа [4].

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 $\langle r, s \rangle$.

Перевіряючий (валідатор) при перевірці підпису $\{m, \langle r, s \rangle\}$ 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 наступне співвідношення:

$$r = x_R \bmod n. \quad (1)$$

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 $\langle r, s \rangle$, що проходить перевірку за допомогою відкритого ключа підписувача Q [4].

В запропонованому протоколі атака порушення анонімності може бути здійснена наступним чином. Підписувач А для кожного рядка своєї бази даних повинен обчислити ймовірний засліплюючий параметр α' [5].

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

Рядок бази даних, для якого виконається співвідношення (1), має вказати на емітента повідомлення.

Доведемо, що точка R' завжди збігається з перевіркою точкою R і не залежить від параметрів h', r', s' і, отже, не дає можливості визначити автора документу 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 документу m .

Протокол сліпого підпису на основі ДСТУ ISO/IEC 14888-3:2014 (ECGDSA)

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

Таблиця 1

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

Таблиця 2

Параметри	ECGDSA
Відкритий ключ	$Q = d^{-1} \cdot G \bmod n$
Точка E	$E = k \cdot G \bmod n = (x_E, y_E)$
Геш-значення	$e = h(m)$
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	$h' = \frac{r'}{r} \cdot \frac{h}{\alpha} \bmod n$
Параметр для перевірки на анонімність	$\alpha' = \frac{s}{s' \cdot \frac{r}{r'}} \bmod n, \alpha' = \frac{r}{r'} \cdot \frac{h}{h'} \bmod n$
Перевірка на анонімність	$R' = \alpha' \cdot E \bmod n = (x_{R'}, y_{R'}) \Rightarrow$ $R' = (\frac{h}{r} \cdot G + \frac{s}{r} \cdot Q) \bmod n, r = x_{R'} \bmod n$

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

$$s = s' \cdot \frac{r}{r'} \cdot \alpha \bmod n. \quad (2)$$

Перевіряючий (валідатор) при перевірці підпису $\{m, \langle r, s \rangle\}$ обчислює точку R , для чого використовує відкритий ключ Q підписувача А:

$$R = (\frac{h}{r} \cdot G + \frac{s}{r} \cdot Q) \bmod n = (x_R, y_R). \quad (3)$$

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

$$\begin{aligned}
 R &= (\frac{h}{r} \cdot G + \frac{s}{r} \cdot Q) \bmod n = (\frac{h}{r} \cdot G + \frac{s' \cdot \frac{r}{r'} \cdot \alpha}{r} \cdot Q) \bmod n = \\
 &= (\frac{h}{r} \cdot G + \frac{\frac{r}{r'} \cdot \alpha (kr' - h')d}{r} \cdot Q) \bmod n = (\frac{h}{r} \cdot G + \frac{\alpha r d (k - \frac{h}{r\alpha})}{r} \cdot Q) \bmod n = \\
 &= (\frac{h}{r} \cdot G + \frac{\alpha k r d}{r} \cdot \frac{G}{d} - \frac{h d}{r} \cdot \frac{G}{d}) \bmod n = \alpha E \bmod n = (x_R, y_R) = C = (x_C, y_C).
 \end{aligned} \quad (4)$$

В 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

$$\alpha' = \frac{s}{s' \cdot \frac{r}{r'}} \bmod n \quad (5)$$

- виходячи з формули засліпленого геш-значення

$$\alpha' = \frac{r}{r'} \cdot \frac{h}{h'} \bmod n \quad (6)$$

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

$$R' = \alpha' \cdot E \bmod n = (x_{R'}, y_{R'}) \quad (7)$$

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

$$\begin{aligned} R' &= \alpha' \cdot E \bmod n = kG \frac{r'h}{rh} \bmod n = kG \left(\frac{(h' + d^{-1}s')h}{rh'} \right) \bmod n = \\ &= \frac{(h' + d^{-1}s')h}{rh'} \cdot G \bmod n = \left(\frac{h}{r} \cdot G + \frac{r'h}{rh'} \cdot Q \right) \bmod n = \\ &= \left(\frac{h}{r} \cdot G + \frac{1}{r} \left(s' \cdot \frac{h}{h'} \right) \cdot Q \right) \bmod n = \left(\frac{h}{r} \cdot G + \frac{s}{r} \cdot Q \right) \bmod n. \end{aligned} \quad (8)$$

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

Протокол сліпого підпису на основі ДСТУ ISO/IEC 14888-3:2014 (ECKCDSA)

У табл. 3 та 4 наведено параметри протоколу сліпого підпису на основі алгоритму цифрового підпису ECKCDSA [1].

Таблиця 3

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

Таблиця 4

Параметри	ECKCDSA
Відкритий ключ	$Q = d^{-1} \cdot G \bmod n$
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'	$r = H(x_C \parallel y_C) \bmod n, r' = H(x_E \parallel y_E) \bmod n$
Засліплений геш-образ	$h' = \frac{r \oplus h}{\alpha} \oplus r' \bmod n$
Параметр для перевірки на анонімність	$\alpha' = \frac{s}{s'} \bmod n, \alpha' = \frac{r \oplus h}{r' \oplus h'} \bmod n$
Перевірка на анонімність	$R' = \alpha' \cdot E \bmod n = (x_{R'}, y_{R'}) \Rightarrow, r = x_{R'} \bmod n$ $R' = (e \cdot G + s \cdot Q) \bmod n$

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

$$s = s' \cdot \alpha \bmod n. \quad (9)$$

Перевіряючий (валідатор) при перевірці підпису $\{m, \langle r, s \rangle\}$ обчислює точку R , для чого використовує відкритий ключ Q підписувача А:

$$R = \left(\frac{h}{r} \cdot G + \frac{s}{r} \cdot Q \right) \bmod n = (x_R, y_R). \quad (10)$$

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

$$\begin{aligned}
 R &= (s \cdot G + r \cdot Q) \bmod n = ((e + dr')\alpha G + rQ) \bmod n = \\
 &= (\alpha eG + \alpha r' dG + rQ) \bmod n = (\alpha E + \alpha h' x_E dG + rQ) \bmod n = \\
 &= (\alpha E + rQ + \alpha Q x_E \frac{x_C \cdot h}{x_E \cdot \alpha}) \bmod n = (\alpha E + rQ + x_C hQ) \bmod n = \\
 &= (\alpha E - rdG + rQ) \bmod n = (\alpha E - rdG + rdG) \bmod n = \\
 &= \alpha E \bmod n = (x_R, y_R) = C = (x_C, y_C).
 \end{aligned} \quad (11)$$

В 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

$$\alpha' = \frac{s}{s'} \bmod n. \quad (12)$$

- виходячи з формули засліпленого геш-значення

$$\alpha' = \frac{r \oplus h}{r' \oplus h'} \bmod n \quad (13)$$

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

$$R' = \alpha' \cdot E \bmod n = (x_{R'}, y_{R'}). \quad (14)$$

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

$$\begin{aligned} R' &= \alpha' \cdot E \bmod n = \alpha' kG \bmod n = \alpha' G \left(\frac{s'}{d} + (r' \oplus h') \right) \bmod n = \\ &= \alpha' G \left(\frac{s'}{d} + e' \right) \bmod n = (\alpha' s' Q + \alpha' e' G) \bmod n = \\ &= (s \cdot Q + (r' \oplus h') \frac{r \oplus h}{r' \oplus h'} \cdot G) \bmod n = (e \cdot G + s \cdot Q) \bmod n. \end{aligned} \quad (14)$$

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

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 вказане, можна стверджувати, що сліпому та остаточному підпису у протоколі сліпого підпису загрожують аналогічні атаки [3]. Але існують і спеціальні атаки, що притаманні лише протоколам сліпого підпису.

Як вказано вище, усі алгоритми проходять перевірку на анонімність і, навіть, якщо підписувач А буде зберігати усі параметри h', r', s' , то в подальшому він не зможе встановити відповідність цих параметрів до емітента, для якого підпис було виконано. Але для наведених алгоритмів є особливість $-\alpha'$ виражається двома виразами, які будуть приймати однакове значення лише для абонента В, що формував остаточний підпис за цими параметрами (ймовірність того, що буде ще один емітент, для якого два вирази α' будуть мати однакове значення, дорівнює 2^{-n}). З цього виходить, що наведений механізм для ЕКГДСА та ЕСКДСА забезпечує сліпий підпис з відстежуємою 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 в 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 засліпленого геш-образу. В такому випадку підписувач А – лише оператор криптомодуля D, який не має прямого доступу до ключів (або D може повністю замінювати А, тоді емітенту В надається доступ до роботи із засобом КЗІ). Виконуються наступні операції:

- 1) абонент В направлено зашифровує h' на відкритому ключі криптомодуля D;
- 2) Отримане $E_D(h')$ надсилається D (прямо чи за допомогою оператора А);
- 3) D розшифровує h' та створює s' ;
- 4) r' та s' відсилаються емітенту В, а h' видаляється з пам'яті D.

Через те, що h' обробляється лише у D і А 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 в хмарах. Також одним з прикладів використання сліпого підпису на основі засобів КЗІ є проведення виборів. Виборці заходять до кабінки, де стоїть автоматизована 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

На основі алгоритмів ЕП, що базуються на стандартах ДСТУ ISO/IEC 14888-3:2014 (ECGDSA, ECKCDSA) [1], принципів побудови протоколів сліпого ЕП [2] було побудовано протокол сліпого електронного підпису.

Основна вимога цих протоколів полягає в тому, що створення підпису та його перевірка виконувалися за стандартними алгоритмами і лише засліплення вимагало б додаткових криптографічних перетворень. Перевага запропонованого методу полягає в тому, що така методика робить впровадження функціоналу сліпого підпису в існуючі інформаційно-телекомунікаційні системи таким, що не потребує додаткових зусиль. Необхідно лише реалізувати протокол для емітента, а підписувач та валідатор можуть використовувати вже існуючі засоби створення та перевірки ЕП.

За результатами дослідження 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 [4, 5].

Також даний метод має переваги при розробці стандартів. Такий підхід дозволяє напряму посилається 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 множить або ділить на випадкове число, яке жодним чином не впливає на стійкість до атак.

Список літератури: 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. Горбенко, І.Д., Горбенко, Ю.І. Прикладна криптологія. Теорія. Практика. Застосування. Харків : Форт, 2012. 870 с. 4. 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. 5. 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.

Харківський національний університет
імені В.Н.Каразіна

Надійшла до редколегії 11.12.2015