НОВІ ЗАСОБИ
КІБЕРНЕТИКИ, ІНФОРМАТИКИ,
ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ
ТА СИСТЕМНОГО АНАЛІЗУ

Г.Л. КОЗІНА, Д.К. САВЧЕНКО

УДК 004.056

ПРОТОКОЛ АГРЕГОВАНОГО ПІДПИСУ З ЛІДЕРОМ ГРУПИ

Анотація. Запропоновано протокол агрегованого електронного цифрового підпису з Лідером групи. Протокол реалізовано в групі точок еліптичної кривої над розширеним полем. Наведено приклад формування підпису на реальному документі.

Ключові слова: криптографічний протокол, електронний цифровий підпис, агрегований підпис, відкритий ключ.

ВСТУП

У сучасному світі комп'ютерних технологій та електронного документообігу застосування електронного цифрового підпису [1, 2] є необхідним для захисту юридичних документів. Існують різні протоколи підпису, які використовуються на практиці. У цій галузі опубліковано багато робіт як іноземних, так і вітчизняних дослідників. У роботах [3–14] розглянуто індивідуальний, сліпий, мультипідпис (або колективний), агрегований (або композиційний), груповий тощо.

В Україні у напрямку розвитку електронного цифрового підпису працюють такі науковці: Задірака В.К., Горбенко І.Д., Горбенко Ю.І., Кочубінський А.І., Бессалов А.В., Фаль О.М. та ін. Наприклад, у роботі [13] розглянуто алгоритм обчислення сліпого цифрового мультипідпису на основі стандарту ДСТУ 4145-2002. В обчисленні сліпого цифрового мультипідпису беруть участь група рівноправних суб'єктів та координатор групи, який забезпечує взаємодію членів групи. При цьому координатор групи виконує обчислення без використання секретних параметрів.

У цій роботі запропоновано новий протокол агрегованого цифрового підпису з Лідером групи.

Згідно з роботою [5], підпис називають агрегованим, якщо кожен учасник групи підписантів підписує кожний свій документ, а потім всі індивідуальні підписи агрегують в єдиний підпис, розмір якого є значно меншим сумарного розміру індивідуальних підписів. Особливістю запропонованого протоколу є те, що в обчисленні агрегованого підпису беруть участь група підписантів, які не є рівноправними, та Лідер групи. Лідер не тільки координує процес підписання, він

також створює єдиний документ, частини якого надають учасникам групи для підписання. Цей документ також підписує Лідер за допомогою свого секретного ключа.

Лідер формує кінцевий підпис на основі індивідуальних підписів учасників групи та свого підпису. Для перевірки агрегованого підпису використовуються відкриті ключі всіх підписантів та Лідера групи. При цьому частини документу, які підписують учасники групи, також додаються до основного документа. Формування протоколу агрегованого підпису з такими якостями є необхідним для забезпечення схожості процедури підписання електронних документів з паперовими документами, які потрібно підготувати, підписати та затвердити.

ПРОТОКОЛ АГРЕГОВАНОГО ЦИФРОВОГО ПІДПИСУ ЕЛЕКТРОННОГО ДОКУМЕНТА З ЛІДЕРОМ У ГРУПІ ТОЧОК ЕЛІПТИЧНОЇ КРИВОЇ

У цьому протоколі використовуються дві функції перетворень:

$HB2I_l(x)$ — перетворення l молодших бітів з бітової послідовності x у ціле число;

$FE2I_l(x)$ — перетворення l молодших бітів з бітової послідовності, що відповідає елементу поля x, у ціле число.

Загальносистемні параметри. Вони є такими: еліптична крива над скінченним полем $GF(2^m)$ з примітивним многочленом $f(t)$ степеня m

$$y^2 + xy = x^3 + Ax^2 + B,$$

де $A, B \in GF(2^m)$, $\mathrm{A} \in \{0,1\}$, $B \neq 0$, разом із приєднаною нескінченно віддаленою точкою O; базова точка еліптичної кривої $P \neq \mathrm{O}$ простого порядку n така, що $nP = \mathrm{O}$ і $kP \neq \mathrm{O}$, $0 < k < n$, $|n|$ — довжина n у бітах; $H(\cdot)$ — обрана функція гешування, наприклад, відповідно до стандарту ДСТУ 7564-2014; δ — допоміжне просте число (введення допоміжного числа δ дає змогу скоротити першу частину цифрового підпису).

Генерація ключів. Кожний потенційний представник групи A_i, $i = 1, 2, \ldots, t$, має асиметричну пару ключів: особистий d_i та відкритий $Q_i = -d_i P$, $1 < d_i < n$. Лідер групи також має асиметричну пару ключів: особистий d_L та відкритий $Q_L = -d_L P$, $1 < d_L < n$.

Формування цифрового підпису. Нехай Лідер сформував електронний документ M, групу із t представників та відповідні частини $\{M_1, M_2, \ldots, M_t\}$ документа M, причому кожен користувач i, $i = 1, 2, \ldots, t$, має підписати свій електронний документ M_i з геш-образом $H(M_i)$, а Лідер підписує документ M з геш-образом $H(M)$. Геш-образи документів $H(M)$, $H(M_i)$, $i = 1, 2, \ldots, t$, перетворюють за допомогою функції $HB2I_l(x)$ у цілі числа $h = HB2I_{|n|-1}(H(M))$, $h_i = HB2I_{|n|-1}(H(M_i))$ відповідно. Кожен представник групи вибирає одноразовий випадковий секретний ключ k_i, $1 < k_i < n$, обчислює точку еліптичної кривої

$$R_i = k_i P \tag{1}$$

та надає її Лідеру для подальшого використання. Лідер також вибирає одноразовий випадковий секретний ключ k_L, $1 < k_L < n$, обчислює точку

$$R_L = k_L P$$

та суму всіх точок R_i , $i = 1, 2, \ldots, t$, і R_L

$$R = \sum_{i=1}^{t} R_i + R_L = (xR,\ yR)\,, \tag{2}$$

після чого формується перший елемент агрегованого підпису — число r.

Число r обчислюють за формулою

$$r = FE2I_{|n|-1}(xR) \cdot h \bmod \delta, \tag{3}$$

при цьому воно не повинно дорівнювати нулю. Для $r = 0$ вибирають нові випадкові секретні ключі k_i. Потім кожний представник групи A_i за допомогою секретного ключа d_i, значення k_i та числа h_i, відповідного геш-образу документа M_i, обчислює підпис $\langle r_i, s_i \rangle$:

$$r_i = r \cdot h_i \bmod n\,, \quad s_i = k_i + r \cdot d_i \cdot h_i \bmod n \tag{4}$$

та надає його Лідеру. Кожен представник групи надає Лідеру свій відкритий ключ Q_i. Лідер перевіряє справжність кожного підпису $\langle r_i, s_i \rangle$ за допомогою відповідного відкритого ключа підписанта Q_i. Якщо виконується співвідношення

$$s_i P + r_i \cdot Q_i = R_i\,, \tag{5}$$

підпис визнають справжнім. Далі Лідер за допомогою секретного ключа d_L, значення k_L та числа h, відповідного геш-образу документа M, обчислює підпис $\langle r_L, s_L \rangle$:

$$r_L = r \cdot h \bmod n\,, \quad s_L = k_L + r_L \cdot h \bmod n, \tag{6}$$

після чого генерується число s — другий елемент підпису:

$$s = \left(s_L + \sum_{i=1}^{t} s_i \right) \bmod n. \tag{7}$$

Число s не може дорівнювати нулю. Для $s = 0$ процедуру підписання повторюють. Агрегованим підписом кортежу документів $\{M_1, M_2, \ldots, M_t, M\}$ є двійка $\langle r, s \rangle$.

Перевірка цифрового підпису. Перевірку агрегованого підпису $\langle r, s \rangle$ під кортежем документів $\{M_1, M_2, \ldots, M_t, M\}$ здійснюють за допомогою відкритих ключів $\{Q_1, Q_2, \ldots, Q_t, Q_L\}$ кожного підписанта та Лідера, а також геш-образів наданих документів $H(M_i)$, $H(M)$ і відповідних чисел $h_i = HB2I_{|n|-1}(H(M_i))$, $h = HB2I_{|n|-1}(H(M))$.

Обчислюють точки

$$Q = \sum_{i=1}^{t} h_i \cdot Q_i + h \cdot Q_L, \tag{8}$$

$$RR = sP + r \cdot Q = (xRR,\ yRR)\,. \tag{9}$$

Число $\tilde{r}$ обчислюють за формулою

$$\tilde{r} = FE2I_{|n|-1}(xRR) \cdot h \bmod \delta. \tag{10}$$

Якщо $\tilde{r} = r$, то агрегований цифровий підпис електронних документів $\{M_1, M_2, ..., M_t, M\}$ визнають справжнім.

Покажемо коректність пропонованого алгоритму формування та перевірки агрегованого підпису.

Обчислимо

$$(xRR,\ yRR) = RR = sP + r \cdot Q = \left(s_L + \sum_{i=1}^{t} s_i \right) \cdot P + r \cdot \left(\sum_{i=1}^{t} h_i \cdot Q_i + h \cdot Q_L \right) =$$

$$= \left(k_L + r_L \cdot d + \sum_{i=1}^{t} (k_i + r_i \cdot d_i) \right) \cdot P + r \cdot \sum_{i=1}^{t} h_i \cdot Q_i + r \cdot h \cdot Q_L =$$

$$= R_L + \sum_{i=1}^{t} R_i - r \cdot h \cdot Q_L - r \cdot \sum_{i=1}^{t} h_i \cdot Q_i + r \cdot \sum_{i=1}^{t} h_i \cdot Q_i + r \cdot h \cdot Q_L = R = (xR,\ yR).$$

Оскільки $RR = R$, то $\tilde{r} = r$:

$$\tilde{r} = FE2I_{|n|-1}(xRR) \cdot h \bmod \delta = FE2I_{|n|-1}(xR) \cdot h \bmod \delta = r.$$

Розглянемо можливість підробки Лідером підписаного документа. Оскільки Лідер формує кінцевий кортеж документів, він може сформувати їх на свій розсуд. Для успішної перевірки підпису підроблених документів $\{M_1^*, M_2^*, ..., M_t^*, M^*\}$ потрібно, щоб виконувалась умова $\sum_{i=1}^{t} h_i^* \cdot Q_i + h^* \cdot Q_L = \sum_{i=1}^{t} h_i \cdot Q_i + h \cdot Q_L = Q$, де числа $h_i = HB2I_{|n|-1}(H(M_i))$, $h = HB2I_{|n|-1}(H(M))$ відповідають геш-образам $H(M_i)$, $H(M)$ документів $\{M_1, M_2, ..., M_t, M\}$, які пройшли перевірку, а $h_1^*, h_2^*, ..., h_t^*, h^*$ є відповідними геш-образам підроблених документів $\{M_1^*, M_2^*, ..., M_t^*, M^*\}$.

Звідси

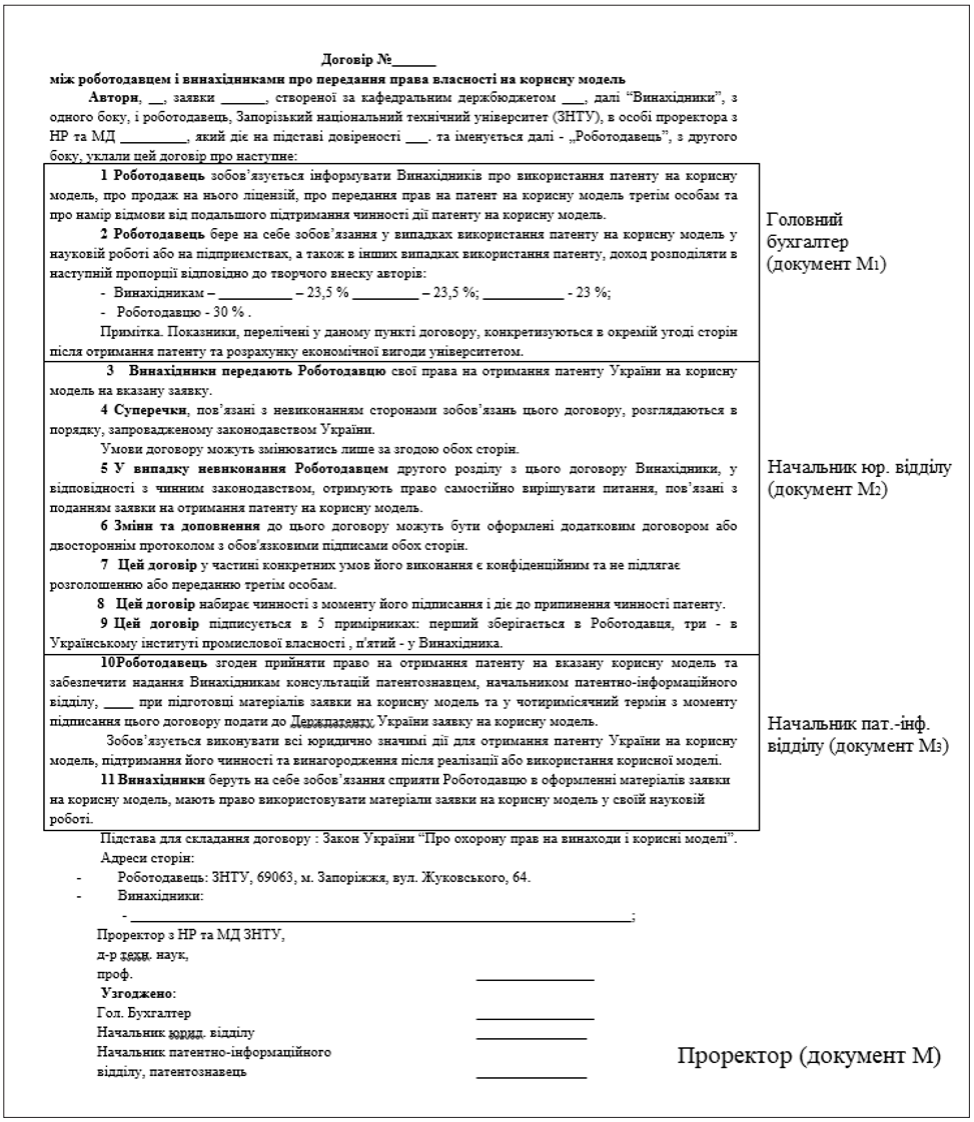
$$h^* \cdot Q_L = Q - \sum_{i=1}^{t} h_i^* \cdot Q_i = Q^*.$$

Для успішної атаки Лідеру потрібно розв'язати задачу дискретного логарифмування в групі точок еліптичної кривої над розширеним полем відносно h^*:

$$h^* \cdot Q_L = Q^*$$

та знайти «правильний» документ M^* з геш-образом, який відповідає числу $h^* = HB2I_{|n|-1}(H(M^*))$. Обидві ці задачі є важкорозв'язними. До того ж, під час формування першої частини підпису r використовують число h, яке відповідає за цілісність документа M.

Зрозуміло, що у випадку слабкості формули підпису можна підробити підпис без участі легального підписанта. Автори цієї статті будуть вдячні, якщо читачі нададуть приклади успішних атак на запропоновану формулу підпису.



Договір №_____

між роботодавцем і винахідниками про передання права власності на корисну модель

Автори, __, заявки _____, створеної за кафедральним держбюджетом ___, далі "Винахідники", з одного боку, і роботодавець, Запорізький національний технічний університет (ЗНТУ), в особі проректора з НР та МД _____, який діє на підставі довіреності ___. та іменується далі - „Роботодавець", з другого боку, уклали цей договір про наступне:

1 Роботодавець зобов'язується інформувати Винахідників про використання патенту на корисну модель, про продаж на нього ліцензій, про передання прав на патент на корисну модель третім особам та про намір відмови від подальшого підтримання чинності дії патенту на корисну модель.

Головний бухгалтер (документ М1)

2 Роботодавець бере на себе зобов'язання у випадках використання патенту на корисну модель у науковій роботі або на підприємствах, а також в інших випадках використання патенту, доход розподіляти в наступній пропорції відповідно до творчого внеску авторів:

- Винахідникам – _____ – 23,5 % _____ – 23,5 %; _____ - 23 %;
- Роботодавцю - 30 % .

Примітка. Показники, перелічені у даному пункті договору, конкретизуються в окремій угоді сторін після отримання патенту та розрахунку економічної вигоди університетом.

3 Винахідники передають Роботодавцю свої права на отримання патенту України на корисну модель на вказану заявку.

4 Суперечки, пов'язані з невиконанням сторонами зобов'язань цього договору, розглядаються в порядку, запровадженому законодавством України.

Умови договору можуть змінюватись лише за згодою обох сторін.

5 У випадку невиконання Роботодавцем другого розділу з цього договору Винахідники, у відповідності з чинним законодавством, отримують право самостійно вирішувати питання, пов'язані з поданням заявки на отримання патенту на корисну модель.

Начальник юр. відділу (документ М2)

6 Зміни та доповнення до цього договору можуть бути оформлені додатковим договором або двосторонніми протоколом з обов'язковими підписами обох сторін.

7 Цей договір у частині конкретних умов його виконання є конфіденційним та не підлягає розголошенню або переданню третім особам.

8 Цей договір набирає чинності з моменту його підписання і діє до припинення чинності патенту.

9 Цей договір підписується в 5 примірниках: перший зберігається в Роботодавця, три - в Українському інституті промислової власності , п'ятий - у Винахідника.

10Роботодавець згоден прийняти право на отримання патенту на вказану корисну модель та забезпечити надання Винахідникам консультацій патентознавцем, начальником патентно-інформаційного відділу, ____ при підготовці матеріалів заявки на корисну модель та у чотиримісячний термін з моменту підписання цього договору подати до Держпатенту України заявку на корисну модель.

Начальник пат.-інф. відділу (документ М3)

Зобов'язується виконувати всі юридично значимі дії для отримання патенту України на корисну модель, підтримання його чинності та винагородження після реалізації або використання корисної моделі.

11 Винахідники беруть на себе зобов'язання сприяти Роботодавцю в оформленні матеріалів заявки на корисну модель, мають право використовувати матеріали заявки на корисну модель у своїй науковій роботі.

Підстава для складання договору : Закон України "Про охорону прав на винаходи і корисні моделі".

Адреси сторін:

- Роботодавець: ЗНТУ, 69063, м. Запоріжжя, вул. Жуковського, 64.
- Винахідники:
  - _____;

Проректор з НР та МД ЗНТУ,
д-р техн. наук,
проф. _____

Узгоджено:
Гол. Бухгалтер _____
Начальник юрид. відділу _____
Начальник патентно-інформаційного відділу, патентознавець _____

Проректор (документ М)

Рис. 1. Електронний документ для підписання

Приклад 1. Нехай потрібно підписати договір між роботодавцем і винахідниками про передачу права власності на корисну модель під час оформлення заявки на патент.

У підписанні цього документа беруть участь три члени групи та Лідер. Лідер формує електронний документ до підпису, визначає частини документа та надає їх відповідним членам групи. Кожний член групи підписує свою частину документа. У цьому прикладі це головний бухгалтер, начальник юридичного відділу та начальник патентно-інформаційного відділу. Лідер (Проректор) після підписання кожним учасником своєї частини документа підписує його і цим засвідчує підписи членів групи.

На рис. 1 виділено частини документів, які підписують члени групи та Лідер.

Виберемо такі загальні параметри.

1. Основне поле — скінченне поле $GF(2^{163})$, $f(t) = t^{163} + t^7 + t^6 + t^3 + 1$; еліптична крива над основним полем

$$y^2 + xy = x^3 + Ax^2 + B,$$

$$A, B \in GF2^{163}, A \in \{0,1\},$$

$$B = 87654647262729695669716335333426868668597192205 13,$$

елементи поля $GF(2^{163})$ у прикладі 1 відображено цілими числами.

Число точок цієї еліптичної кривої дорівнює простому числу 5846006549323611672814742649529786791204665225549, тобто будь-яка її точка має порядок $n = 5846006549323611672814742649529786791204665225549$, $|n| = 163$.

2. Базова точка еліптичної кривої

$$P = \begin{pmatrix} 1049041545936676220972032861684343064186929990 9664, \\ 1957695503604687263794263659666036499214093510 67 \end{pmatrix}.$$

3. Допоміжне просте число $\delta = 1125899839733759$.

Нехай число користувачів $t = 3$. Відповідні особисті ключі учасників групи є такими:

$$d_1 = 25178254896074825,$$

$$d_2 = 584698554574845548766339451548745620154012,$$

$$d_3 = 125787451354805468174125954782415 3.$$

Тоді відкриті ключі є такими:

$$Q_1 = \begin{pmatrix} 256894482824133445082207432708438408332981338215 9, \\ 121141443473687186044315003946179452614181804645 5 \end{pmatrix},$$

$$Q_2 = \begin{pmatrix} 936115696670772146770257477473469548362082706758 8, \\ 692617539260694240778664882087051819190329981619 2 \end{pmatrix},$$

$$Q_3 = \begin{pmatrix} 761388883872516654293885547185201885893977364787 4, \\ 391019700538576982022308357171358175293021632075 0 \end{pmatrix}.$$

Лідер групи також має асиметричну пару ключів: особистий

$$d_L = 221486679435618357018555322993898795570929043718 2$$

та відкритий

$$Q_L = \begin{pmatrix} 802630562082779602032520800826167545983150311087 4, \\ 571086997417084484289661255591514822962370122385 0 \end{pmatrix}.$$

Далі обчислюють геш-образи (геш-функція SHA-256) документів $\{M_1, M_2, M_3, M\}$:

$$H(M_1) = 57feb9b7bbdcd02b34c652464638ca3181e584fb31ef0c888d093edf2b0dbb1e$$
$$H(M_2) = d9e18d301aae802bff6a24d30756a004e9476a1ec5cc1e7a055f46147a3037f3$$
$$H(M_3) = d68ee2855375eb1aefb3b02f7860bbcbca7b230f761467b4b6fec5bbce569dd9$$
$$H(M) = 95b753aeef774ef50bee5e8d91f87c589e0c927512701cc58a08a9d9043f05712$$

та відповідні десяткові числа $h_i = HB2I_{|n|-1}(H(M_i))$:

$$h_1 = 33238990838788486573120719190065690693128891748 14,$$
$$h_2 = 44263996511125087426623954361194000244477767331 71,$$
$$h_3 = 50717410353745615802287054492330003023785271372 41,$$
$$h = 16415081598660479226840929455461927407815166748 34.$$

Кожний представник групи вибирає одноразовий випадковий секретний ключ k_i:

$$k_1 = 21542012478452124510369459452021,$$
$$k_2 = 32015241505412896584842 31,$$
$$k_3 = 541209867454102310,$$

обчислює координати точки R_i:

$$R_1 = \begin{pmatrix} 52163092624876971927276502000045694286942447662 15, \\ 89878956480162020239253805195706561274993586443 16 \end{pmatrix},$$

$$R_2 = \begin{pmatrix} 62203844960480419114802010528861404620610139563 11, \\ 33905027111651494595003517890415669557863319520 4 \end{pmatrix},$$

$$R_3 = \begin{pmatrix} 57945558475193418785413879345813887907825211332 98, \\ 10667123130313562960250933134812390273456216041331 \end{pmatrix}.$$

та надає Лідеру для подальшого використання.

Лідер також вибирає одноразовий випадковий секретний ключ $k_L = 215479854345870035978412457101$, обчислює точку

$$R_L = \begin{pmatrix} 45212472659978433198388325891909677445670391806 59, \\ 98606329679652058304428853253038685849621555164 5 \end{pmatrix}$$

та суму всіх точок R_i, $i = 1, 2, \ldots, t$, і R_L

$$R = \sum_{i=1}^{t} R_i + R_L = \begin{pmatrix} 61249422641838460747954949268935985928129081556 60, \\ 92074404041894885294300438897000538212286610148 75 \end{pmatrix},$$

після чого формується перший елемент агрегованого підпису — число $r = 642189796165685$. Потім кожний представник групи A_i за допомогою секретного ключа d_i, значення k_i та числа h_i, відповідного геш-образу документа M_i, обчислює підпис $\langle r_i, s_i \rangle$:

$$r_1 = 23101784229562343466097059108130150285115466011 61,$$
$$s_1 = 19921080699008688995426193751976097458189374892 5,$$

$$r_2 = 43880680389508263064470849499027752571194406200 58,$$
$$s_2 = 21362424453103621280125706624111691338113686698 64,$$

$$r_3 = 53947126520198948645989757117402550319799052398 77,$$
$$s_3 = 36755426360353399238180321162194777249514950160 47,$$

та надає Лідеру. Лідер перевіряє справжність кожного підпису $\langle r_i, s_i \rangle$ за допо-

могою відповідного відкритого ключа підписанта Q_i. Оскільки для кожного представника групи виконується $s_i P + r_i \cdot Q_i = R_i$, підпис визнають справжнім. Далі Лідер за допомогою секретного ключа d_L, значення k_L та числа h, відповідного геш-образу документа M, обчислює підпис $\langle r_L, s_L \rangle$:

$$r_L = 358680678447334421168173902466315025942679912659 1,$$
$$s_L = 161490818626332719350377472912080547619567696854,$$

після чого генерується число s — другий елемент підпису:

$$s = 326480157638509988320499539532701589759659906141.$$

Агрегованим підписом є двійка

$$\left\langle \begin{matrix} r = 642189796165685 \\ s = 326480157638509988320499539532701589759659906141 \end{matrix} \right\rangle.$$

Перевірку агрегованого підпису

$$\left\langle \begin{matrix} r = 642189796165685 \\ s = 326480157638509988320499539532701589759659906141 \end{matrix} \right\rangle$$

під кортежем документів $\{M_1, M_2, ..., M_t, M\}$ здійснюють за допомогою відкритих ключів $\{Q_1, Q_2, ..., Q_t, Q_L\}$ кожного підписанта та Лідера, а також геш-образів наданих документів $H(M_i)$, $H(M)$ і відповідних чисел $h_i = HB2I_{|n|-1}(H(M_i))$, $h = HB2I_{|n|-1}(H(M))$.

Особа, яка здійснює перевірку, обчислює точки

$$Q = \sum_{i=1}^{t} h_i \cdot Q_i + h \cdot Q_L = \begin{pmatrix} 3663927011569833876230497510790952399261977649407 \\ 7146070157871668738716430540707553452380599963444 \end{pmatrix}.$$

$$RR = sP + r \cdot Q = \begin{pmatrix} 6124942264183846074795494926893598592812908155660, \\ 9207440404189488529430043889700053821228661014875 \end{pmatrix}$$

і число $\tilde{r} = FE2I_{|n|-1}(xRR) \cdot h \bmod \delta = 642189796165685$.

Оскільки $\tilde{r} = r$, агрегований цифровий підпис електронних документів $\{M_1, M_2, ..., M_t, M\}$ визнають справжнім.

ВИСНОВКИ

Запропонований протокол цифрового агрегованого підпису електронних документів є подібним до процедури підписання паперових документів, які мають бути підписані групою учасників та затверджені керівником.

У запропонованому протоколі загальний розмір агрегованого підпису є значно меншим, ніж сумарний розмір індивідуальних підписів учасників підписання. При цьому першу частину підпису можна зменшити за рахунок вибраного допоміжного простого числа. Це важливо в тих випадках, коли загальний розмір підпису є обмеженим.

Автори вдячні рецензентові за конструктивні та продуктивні зауваження.

СПИСОК ЛІТЕРАТУРИ

1. Задірака В.К., Кудін А.М., Людвиченко В.О., Олексюк О.С. Комп'ютерні технології криптографічного захисту інформації на спеціальних цифрових носіях. Київ–Тернопіль: Підручники і посібники, 2007. 272 с.
2. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Теорія. Практика. Застосування. Вид. 2-е. Харків : ФОРТ, 2012. 878с.
3. Кочубинский А.И., Фаль А.М. Алгоритмы вычисления слепой цифровой подписи на основе стандарта ДСТУ 4145-2002 и российского стандарта цифровой подписи ГОСТ Р 34. 10-2001. *Кибернетика и системный анализ*. 2012. Т. 48, № 4. С. 95–100.
4. Козіна Г.Л., Молдов'ян М.А., Неласа Г.В. Криптопротоколи: схеми цифрового підпису. Запоріжжя: ЗНТУ, 2014. 152 с.
5. Boneh D., Gentry C., Lynn B., Shacham H. Aggregate and verifiably encrypted signatures from bilinearmaps. *Proc. International Conference on the Theory and Applications of Cryptographic Techniques "Advances in Cryptology EUROCRYPT 2003*" (4–8 May, 2003, Warsaw, Poland). Warsaw, 2003. P. 416–432.
6. Макаров А.О. Схема пост-квантовой агрегированной подписи на основе теории алгебраического кодирования. *Вопросы кибербезопасности*. 2019. № 2 (30). С. 69–76. https://doi.org/10.21681/2311-3456-2019-2-69-76.
7. Zhao Y. Aggregation of gamma-signatures and applications to bitcoin. 2018. URL: https://eprint.iacr.org/2018/414/20180510:203542.
8. Chaum D., van Heyst E. Group signatures. *Proc. Workshop on the Theory and Application of Cryptographic Techniques* "Advances in Cryptology EUROCRYPT 91", *Lecture Notes in Computer Science* (8–11 April, 1991, Brighton, UK). Brighton, 1991. Vol. 547. P. 257–265. http://doi.org/10.1007/3-540-46416-6_22.
9. Micali S., Ohta K., Reyzin L. Accountable-subgroup multisignatures: Extended abstract. *ACM CCS 01*: *Proc. 8th Conference on Computer and Communications Security* (5–8 November, 2001, Philadelphia, USA). Philadelphia, USA, 2001. P. 245–254.
10. Neven G. Efficient sequential aggregate signed data. *Proc. 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques* "*Advances in Cryptology — EUROCRYPT 2008*", *Lecture Notes in Computer Science* (13–17 April, 2008, Istanbul, Turkey). Istanbul, Turkey, 2008. Vol. 4965. P 52–69.
11. Alamelou Q., Blazy O., Cauchie S., Gaborit P. A code-based group signature scheme. *Proc. 9th International Workshop on Coding and Cryptography 2015* (*WCC2015*) (13-17 April 2015, Paris, France). Paris, France, 2015. P. 1–18. URL: https://hal.inria.fr/hal-01276464.
12. Молдовян А.А., Молдовян Н.А., Латышев Д.М., Головачев Д.А. Протокол групповой цифровой подписи на основе маскирования открытых ключей. *Вопросы защиты информации*. 2011. № 3. С. 2–6.
13. Кочубинский А.И., Молдовян Н.А., Фаль А.М. Слепые мультиподписи на основе стандартов ДСТУ 4145-2002 и ГОСТ Р 34. 10-2001. *Reports of the National Academy of Sciences of Ukraine*. 2012. № 3. С. 38–44.
14. Бессалов А.В., Телиженко А.Б. Криптосистемы на эллиптических кривых: Учеб. пособие. Київ: ІВЦ «Видавництво «Політехніка», 2004. 224 с.

Надійшла до редакції 25.07.2019

Г.Л. Козина, Д.К. Савченко

ПРОТОКОЛ АГРЕГИРОВАННОЙ ПОДПИСИ С ЛИДЕРОМ ГРУППЫ

Аннотация. Предложен протокол агрегированной электронной цифровой подписи с Лидером группы. Протокол реализован в группе точек эллиптической кривой над расширенным полем. Приведен пример формирования подписи на реальном документе.

Ключевые слова: криптографический протокол, электронная цифровая подпись, агрегированная подпись, открытый ключ.

G. Kozina, D. Savchenko

AGGREGATE SIGNATURE PROTOCOL WITH GROUP LEADER

Abstract. The protocol of aggregated electronic digital signature with the group Leader is proposed. The protocol is implemented in a group of points of an elliptic curve over an extended field. An example of generating a signature on a real document is presented.

Keywords: cryptographic protocol, electronic digital signature, aggregate signature, public key.

Козіна Галина Леонідівна,
кандидат фіз.-мат. наук, доцент, доцент кафедри Національного університету «Запорізька політехніка», e-mail: ainc00@gmail.com.

Савченко Дарина Костянтинівна,
аспірантка Національного університету «Запорізька політехніка», e-mail: d.k.savch@gmail.com.