УДК 004.056.53+004.057.4 Козіна Г.Л., Карпуков Л.М., Піза Д.М., Молдов'ян М.А.

КОЛЕКТИВНЕ ПІДПИСАННЯ РІЗНИХ ДОКУМЕНТІВ НЕРІВНОПРАВНИМИ УЧАСНИКАМИ ПРОТОКОЛУ

Розвиток інфраструктури відкритих ключів в Україні, створення регіональних центрів сертифікації ключів дозволяє клієнтам отримати та надавати послуги електронного цифрового підпису [1]. Крім класичної схеми однократного цифрового підпису існують інші схеми, зокрема колективний цифровий підпис.

На сьогодні з'явилися нові схеми колективного цифрового підпису в різних постановах. Наприклад, колективний цифровий підпис може бути сформований під одним електронним документом, який завіряє деяка група осіб [2,3] (підписання договорів різними рівноправними учасниками). Кожен учасник створює свою частину підпису, здійснюється обмін відкритими параметрами по мережах зв'язку, після чого формується колективний підпис. Для перевірки колективного підпису формується колективний відкритий ключ, який залежить від відкритих ключів учасників підписання електронного документа.

Однак, якщо учасники підписання не є рівноправними, може виникнути необхідність підписання різних документів групою осіб, кожна із котрих має право підписувати тільки свій документ. Наприклад, директор, бухгалтер, завідувач відділу кадрів, технолог підписують кожний свій електронний документ с використанням свого особистого ключа. С метою зменшення довжини підпису пропонується формування єдиного, колективного підпису різних документів на базі елементів особистих підписів. Перевірка такого колективного підпису потребує знання відкритих ключів кожного із учасників підписання і відповідних кожному електронних документів.

В статті пропонується реалізація протоколів колективного цифрового підпису різних документів на базі стандарту електронного цифрового підпису ДСТУ 4145-2002 [4] і з використанням операцій в простому полі [5].

Протокол колективного цифрового підпису різних документів на базі стандарту електронного цифрового підпису ДСТУ 4145-2002

Загальні параметри стандарту ДСТУ 4145-2002:

основне поле – скінченне поле $GF(2^m)$, яке є розширенням степеня m поля GF(2);

m – просте число в інтервалі [163, 509];

еліптична крива над основним полем

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

де $A, B \in GF(2^m)$, $B \neq 0$, $A \in \{0,1\}$, разом із приєднаною нескінченно віддаленою точкою O;

базова точка еліптичної кривої $P \neq O$ простого порядку n, така що $nP=O$ і $kP \neq O$, $0<k<n$;

H(•) — функція хешування, припустимо використання стандарту [6] та інших.

Генерація ключів

Кожний і-ий (i = 1, 2, …, t) користувач має два ключа:

особистий (секретний) $1 < d_i < n$ та відкритий

$$Q_i = -d_i P.$$

Формування колективного підпису

Нехай користувач i, i = 1, 2, …, t, підписує електронний документ M_i з геш-образом H_i. В бітовому вигляді геш-образу Hі використовуються молодші $|n| - 1$ розряди, які формують десяткове число h_i.

Кожний підписувач обирає одноразовий випадковий секретний ключ k_i, $1 < k_i < n$, обчислює координати точки

$$R_i = k_i P$$

та надає їх для колективного використання.

Далі обчислюється сума всіх точок R_i, i = 1, 2, …, t:

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

після чого формується

$$r = xR \bmod n$$

– перше число колективного електронного цифрового підпису. При $r = 0$ обираються нові випадкові секретні ключи k_i.

Потім кожний користувач і за допомогою свого секретного ключа d_i та значення k_i обчислює свою долю підпису

$$s_i = (k_i + d_i\, h_i\, r) \bmod n,$$

після чого генерується s – друге число колективного електронного цифрового підпису

$$s = \sum_{i=1}^{t} s_i \bmod n.$$

Параметр підпису s не може бути рівним 0. При $s = 0$ процедура підпису повторюється.

Колективним підписом є пара чисел (r, s).

Перевірка колективного підпису

Перевірка підпису здійснюється за допомогою додаткової точки еліптичної кривої

$$Q = \sum_{i=1}^{t} h_i Q_i,$$

яка залежить від відкритих ключів Q_i учасників підписання і відповідних геш-образів електронних документів h_i.

Обчислюється точка R' еліптичної кривої

$$R' = sP + rQ = (xR', yR')$$

після чого формується

$$r' = xR' \bmod n.$$

Якщо $r' = r$, колективний цифровий підпис різних документів M_i, i = 1, 2, …, t, признається справжнім.

Покажемо коректність пропонованого алгоритму формування і перевірки колективного підпису:

$$R' = sP + rQ = \left(\sum_{i=1}^{t} s_i\right)P + r\left(\sum_{i=1}^{t} h_i Q_i\right) = \left(\sum_{i=1}^{t} k_i + d_i h_i r\right)P + r\left(\sum_{i=1}^{t} h_i(-d_i P)\right) = \left(\sum_{i=1}^{t} k_i\right)P = \sum_{i=1}^{t} R_i = R$$

Оскільки $R' = R$, то і $r' = r$.

Приклад роботи протоколу колективного цифрового підпису різних документів

Оберемо загальні параметри відповідно стандарту ДСТУ 4145-2002:

основне поле – скінченне поле $GF(2^{163})$;

еліптична крива над основним полем $y^2 + xy = x^3 + Ax^2 + B$,

$A = 1$, B = `5FF6108462A2DC8210AB403925E638A19C1455D21`;

базова точка еліптичної кривої

P = (`7D`, `4ED6F4E822394A68280E0FB970141836354F3A91C`);

порядок базової точки

n = `400000000000000000002BEC12BE2262D39BCF14D`.

Генерація ключів.
Нехай число користувачів t=3. Відповідні секретні ключі є

d_1 = `3FD35EB7CE4F03AD82BB6D2`
d_2 = `13672B1490E5D5489F4B87`
d_3 = `11DF05AC8F8C6D68E3980D1`.

Тоді відкрити ключі:

Q_1 = (`487453D2214684B2DAE4C1CC71E9E3EFCAC88C92D`, `69795D60DEFC9A16F030A263410956D375B5B037A`)

Q_2 = (`50E57454230C9561A9CBCFFC83106344F0F1E0B27`, `63C72C5B04DA3403FB25DA6087252615B6AAFEA8A`)

Q_3 = (`3807F2C265E68A922C7D7B0446F5280395F1A4927`, `52805BA4AAA49EAD23CAADC98B661918A15C4F442`)

Формування колективного підпису
Нехай геш-образи відповідних документів
h_1 = `21C230E5C8C262B440608E8`
h_2 = `1C626836D58154B65580012`
h_3 = `19599F3265E53C16D7000B9`
Кожний підписувач обирає одноразовий випадковий секретний ключ k_i,
k_1 = `B2B6391DF149F75BAF0B6D2`
k_2 = `2DC76FBC5DE7A15F93315`
k_3 = `58D64BFA7C579B51B8A3D`
та обчислює координати точки R_i

R_1 = (`3414ABBA613ED416B196128C035F4CA4CCB21CDEB`, `754FBC2C79CBCD611EAB81F864CF2F1B8A9AB0CA7`)

R_2 = (`6E53AE38B19CC3C84A121A614170BBC364E147F04`, `275E2F0A84A35FDE9DC5A568FC0BF8CC24841B368`)

R_3 = (`1E827FBED97E2D8675A6C186D9F186703E22C0DF6`, `3B26FE08304AA7B196EC81BA62A84FD8603E19990`)

Далі обчислюється сума всіх точок R_i:

R = (`52E438B27721D2C0994C06D1E080ACC43C0DB9A38`, `4BEE5DF62431A88470660D3ED0EA31D2663DFF939`),

після чого формується r – перше число колективного електронного цифрового підпису:

r = `12E438B27721D2C0994BDAE5CDC28A616871EA8EB`.

Потім кожний користувач і за допомогою свого секретного ключа d_i та значення k_i обчислює свою долю підпису :

s_1 = `C7A626802F1252BDBD021547A3C1A77BF5F7DEFE`

s_2 = `34673E30277D23F25BBE72198768F2A02F467DA09`

s_3 = `12596FCD2F145438FC773AF6EC0982A62BD908239`

після чого генерується s – друге число колективного електронного цифрового підпису:
s = `133B106559829D573405A278DAF06D5B46E3349F3`
Колективним підписом є пара чисел
(r, s) = (`12E438B27721D2C0994BDAE5CDC28A616871EA8EB`,
`133B106559829D573405A278DAF06D5B46E3349F3`).

Перевірка колективного підпису

Перевірка підпису здійснюється за допомогою додаткової точки еліптичної кривої Q, яка залежить від відкритих ключів Q_i учасників підписання і відповідних геш-образів електронних документів h_i:

Q = (`52E38E8AC810DC5345234D89EEC2FB440C09C25CE`,
`484926A6E01AFFA37DDEC15062B62E53EAE3BB86A`)

Обчислюється точка R′ еліптичної кривої

sP = (`29ED5AF0480C7D9159A15DB5A6F607E55AC56D781`,
`6A32FF934D611AB404E3FC01E87D8D7E1BADF09C4`)

rQ = (`4E099EC88C1E50045D1AAB71CD0AC5E8504EFF366`,
`691BDE1A476CC99C726572F38023922EE1EC419BA`)

R' (`52E438B27721D2C0994C06D1E080ACC43C0DB9A38`,
`4BEE5DF62431A88470660D3ED0EA31D2663DFF939`)

r' = `12E438B27721D2C0994BDAE5CDC28A616871EA8EB`

Якщо $r' = r$, колективний цифровий підпис різних документів M_i признається справжнім.

Запропонований протокол колективного цифрового підпису може бути інтегровано в існуючу інфраструктуру відкритих ключів.

Протокол колективного цифрового підпису різних документів з використанням операцій в простому полі

Загальні параметри:
p – просте число, таке що $p = Nz^2 + 1$,
N – парне натуральне число, z – просте число, $z > 2^{64}$,
H(•) — функція хешування, припустимо використання стандарту [4] та інших.

Генерація ключів

Кожний і-ий (i = 1, 2, …, t) користувач має два ключа:
особистий (секретний) $1 < x_i < p$ та відкритий

$$y_i = = x_i^z \bmod p.$$

Формування колективного підпису

Нехай користувач i, i = 1, 2, …, t, підписує електронний документ M_i з геш-образом H_i. В бітовому вигляді геш-образу Hi використаються молодші $|p| - 1$ розряди, які формують десяткове число h_i.

Кожний підписувач обирає одноразовий випадковий секретний ключ k_i, $1 < k_i < p$, обчислює

$$r_i = k_i^z \bmod p.$$

та надає їх для колективного використання.

Далі обчислюється добуток всіх R_i, i = 1, 2, …, t:

$$r = \prod_{i=1}^{t} r_i \bmod p,$$

– перше число колективного електронного цифрового підпису. При $r = 0$ обираються нові випадкові секретні ключи k_i.

Потім кожний користувач і за допомогою свого секретного ключа x_i та значення k_i обчислює свою долю підпису

$$s_i = x_i^{rh_i} k_i \bmod p,$$

після чого генерується s – друге число колективного електронного цифрового підпису

$$s = \prod_{i=1}^{t} s_i \bmod p.$$

Параметр підпису s не може бути рівним 0. При $s = 0$ процедура підпису повторюється.

Колективним підписом є пара чисел (r, s).

Перевірка колективного підпису

Перевірка підпису здійснюється за допомогою додаткового числа

$$y = \prod_{i=1}^{t} y_i^{h_i} \bmod p,$$

яке залежить від відкритих ключів y_i учасників підписання і відповідних геш-образів електронних документів h_i.

Якщо

$$s^z = (y^r \cdot r) \bmod p,$$

колективний цифровий підпис різних документів M_i, i = 1, 2, …, t, признається справжнім.

Покажемо коректність пропонованого алгоритму формування і перевірки колективного підпису:

$$s^z = \left(\prod_{i=1}^{t} s_i\right)^z \bmod p = \left(\prod_{i=1}^{t} x_i^{zh_i}\right)^r \left(\prod_{i=1}^{t} k_i\right)^z \bmod p = \left(\prod_{i=1}^{t} y_i^{h_i}\right)^r \cdot \left(\prod_{i=1}^{t} r_i\right) \bmod p = (y^r \cdot r) \bmod p.$$

Приклад роботи протоколу колективного цифрового підпису різних документів

Оберемо загальні параметри:

p = 5016532319260500262833579836643990377764 1,

z = 35413741398151157021.

Генерація ключів

Нехай число користувачів t=3. Відповідні секретні ключі є
$x_1 = 156758769780$,
$x_2 = 57869879875$,
$x_3 = 87697098098098$.

Тоді відкрити ключі:
$y_1 = 10888347551054112724481415051902837765574$,
$y_2 = 48485941766163329949274968777985639618768$,
$y_3 = 337313283350073087858297931171526744770 75$.

Формування колективного підпису
Нехай геш-образи відповідних документів
$h_1 = 1754698098876532$,
$h_2 = 14356475686824$,
$h_3 = 3465867599709$.
Кожний підписувач обирає одноразовий випадковий секретний ключ k_i,
$k_1 = 42344769879$,
$k_2 = 11809875644$,
$k_3 = 20457089$
та обчислює значення r_i

$r_1 = 104380920996864642527808961295154350486 97$,
$r_2 = 120815396109446983576851710162560133924 43$,
$r_3 = 420214313680268422917436879184120552367 88$.

Далі обчислюється добуток всіх r_i:

$r = 889698798082340056151415969113810482724 4$

– перше число колективного електронного цифрового підпису.

Потім кожний користувач і за допомогою свого секретного ключа x_i та значення k_i обчислює свою долю підпису :

$s_1 = 45725823840994203644906181284301023362599$,
$s_2 = 23734973385614987164918223107345158206628$,
$s_3 = 50162056813870998489648526071915537056 57$,

після чого генерується s – друге число колективного електронного цифрового підпису:

$s = 119487869417321764321639584998536932842 23$.

Колективним підписом є пара чисел

$(r, s) = (889698798082340056151415969113810482724 4$,
$119487869417321764321639584998536932842 23)$.

Перевірка колективного підпису

Перевірка підпису здійснюється за допомогою додаткового значення y, яке залежить від відкритих ключів y_i учасників підписання і відповідних геш-образів електронних документів h_i:

y = 370054869593657064008648476069023004695l6.

Обчислюються

$s^z \bmod p$ = 389125211184713920426199021649714715513 71

та $(y^r \cdot r) \bmod p$ = 389125211184713920426199021649714715513 71.

Оскільки $s^z = (y^r \cdot r) \bmod p$, колективний цифровий підпис різних документів M_i признається справжнім.

Запропонований протокол колективного цифрового підпису не потребує апарату еліптичних кривих и може бути використаний в корпоративних мережах зв'язку.

Дослідження криптостійкості протоколів є наступною метою авторів.

Список літератури

1. Смарт Н. Криптография. - М.: Техносфера, 2005. – 528 с.

2. Артамонов А.В. Применение алгоритма Шнорра в протоколе коллективной подписи / Артамонов А.В., Маховенко Е.Б.// Материалы XIV Всероссийской научной конференции «Проблемы информационной безопасности в системе высшей школы». – 2007. – С. 17-18.

3. Гортинская Л.В. Реализация протоколов коллективной подписи на основе стандартов ГОСТ 34.310–95 и ДСТУ 4145-2002 / Гортинская Л.В., Молдов'ян Н.А., Козина Г.Л. // Правове, нормативне та метрологичне забезпечення системи захисту інформації в Україні. – 2007. – №.2(15). – С.82-86.

4. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що грунтується на еліптичних кривих. Формування та перевіряння: ДСТУ 4145: 2002. – [Чинний від 2002-03-13]. К.: Держстандарт України, 2002. – 38 с.: табл. – (Національний стандарт України).

5. Пат. 31105 Україна, МПК (2006) H03M 5/00, G09C 1/00, H03M 7/00. Спосіб формування і перевірки достовірності колективного електронного цифрового підпису для засвідчення електронного документа / Карпуков Л.М., Козіна Г.Л., Молдов'ян О.А., Молдов'ян М.А.; замовник і патентовласник Запорізький національний технічний університет. – № u200713254; заявл. 28.11.07; опубл. 25.03.08, Бюл. № 6.

6. Информационная технология. Криптографическая защита информации. Функция хэширования: ГОСТ 34.311-95: 1995. - [Чинний від 1998-04-16]. К.: Держстандарт України, 1995. – 12 с. – (Межгосударственный стандарт).

Надійшла 18.02.09