УДК 681.3.06

К.А. ПОГРЕБНЯК, Ю.М. ЛЄНШИНА

Приватне акціонерне товариство "Інститут інформаційних технологій", Харків

ПРОТОКОЛ ХАМЕЛЕОН-ПІДПИСУ НА ОСНОВІ СТАНДАРТУ ДСТУ 4145-2002 З ВИКОРИСТАННЯМ ГЕШ-ХАМЕЛЕОНУ В ГРУПІ ТОЧОК ЕЛІПТИЧНОЇ КРИВОЇ

Пропонується протокол хамелеон-підпису на основі національного стандарту ДСТУ 4145-2002 з використанням геш-хамелеону в групі точок еліптичної кривої, що забезпечує властивості непередаваності підпису та прихованості повідомлення. Обґрунтовується вибір функції гешування у точку на еліптичний кривій, що необхідна для хамелеон-підпису на основі стандарту ДСТУ 4145-2002. Наводяться розгорнуті протоколи спростування підробленого підпису для випадків забезпечення властивості прихованості повідомлення та властивості відновлення повідомлення. Приводиться доведення стійкості запропонованого протоколу геш-хамелеону та хамелеон-підпису.

Ключові слова: *геш-хамелеон, хамелеон-підпис, група точок ЕК, функція відображення, електронний цифровий підпис.*

Вступ

Захист інформації в комп'ютерних системах вимагає комплексного підходу до вибору та застосування механізмів захисту. Однією із важливих але важкорозв'язуваних на практиці завдань є надання кількісних оцінок запропонованим рішенням та обґрунтування їх достатності для протидії існуючим загрозам безпеки інформації. На думку авторів статті найкращим підходом, що може бути застосованим для забезпечення необхідної стійкості механізмів захисту від несанкціонованого доступу є зведення стійкості відповідних послуг до стійкості функцій криптографічної підтримки [1].

Сьогодні єдиним дозволеним до застосування в Україні стандартом електронного цифрового підпису (ЕЦП) є ДСТУ 4145-2002 [2], що ґрунтується на перетвореннях у групі точок еліптичної кривої (ЕК). Цей стандарт може бути застосований для криптографічної підтримки послуг ідентифікації, автентифікації та неспростовності. Зважаючи на те, що в системах, які надають послуги через Інтернет висуваються вимоги до забезпечення анонімності користувачів, актуальної задачею є розробка рішення, яке б надало ДСТУ 4145-2002 властивості, що б розширили сферу застосування стандарту на системи, що вимагають забезпечення приватності. У статті наводяться результати розв'язання задачі вдосконалення ДСТУ 4145-2002 за рахунок розробки геш-хамелеону у групі точок ЕК та його інтеграції до базового ЕЦП. Інтеграція стала можливою, зокрема, завдяки застосуванню функції Icarta у якості геш-функції, що перетворює результат ГОСТ 34.311-95 у точку на ЕК.

1. Розробка протоколу хамелеон-підпису на основі стандарту ДСТУ 4145-2002 з використанням геш-хамелеону в групі точок еліптичної кривої

Протокол хамелеон-підпису на основі стандарту ДСТУ 4145-2002 [2] з використанням геш-хамелеону в групі точок ЕК складається з етапів:

1. Обчислення загальних параметрів хамелеон-підпису.
2. Обчислення одержувачем пари ключів функції геш-хамелеону, після чого відкритий ключ геш-хамелеону передається підписувачу.
3. Обчислення підписувачем пари ключів хамелеон-підпису згідно стандарту ДСТУ 4145-2002, після чого відкритий ключ підпису передається одержувачу підписаного повідомлення.
4. Обчислення цифрового передпідпису згідно стандарту ДСТУ 4145-2002.
5. Обчислення базової функції гешування згідно стандарту ГОСТ 34.311-95.
6. Обчислення функції Icarta [3].
7. Обчислення функції геш-хамелеону [4].
8. Формування хамелеон-підпису.
9. Обчислення колізії одержувачем (необов'язковий)

Розглянемо докладніше деякі з вищезазначених етапів.

На етапі «Обчислення загальних параметрів хамелеон-підпису», обирається еліптична крива:

$$E(F_{2^m}): y^2 + xy = x^3 + Ax^2 + B, \qquad (1)$$

де m – непарне, $A, B \in F_{2^m}$, $B \neq 0$, $A \in \{0,1\}$.

© К.А. Погребняк, Ю.М. Лєншина

Нехай $\#E(F_{2^m}) = q \times cof$, де q – просте число, а $cof \in \{2,4\}$. Визначимо підгрупу $G \subset E(F_{2^m})$ таку, що $G = \langle P \rangle$, де P – елемент групи порядку q.

На етапі «Обчислення відкритого та особистого ключів функції геш-хамелеону» спочатку виконується алгоритм обчислення особистого ключа функції геш-хамелеону наступним чином: одержувач випадковим чином обирає особистий ключ $z \in [1,q]$ та обчислює відкритий ключ як $Y = zP$, дійсність якого засвідчується шляхом включення його до складу сертифікату відкритого ключа одержувача.

Етап «Обчислення відкритого та особистого ключів хамелеон-підпису» виконується згідно стандарту ДСТУ 4145-2002 [2] без будь-яких змін. Особистим та відкритим ключем відповідно будуть випадкове ціле d та точка ЕК вигляду $Q = -dP$, де P – базова точка ЕК, а $d \in [2, m-1]$.

Далі виконується етап «Обчислення цифрового передпідпису» (згідно стандарту ДСТУ 4145-2002 без будь-яких змін). Цифровий передпідпис позначається як (e, F_e), де e – випадкове число, а $F_e = x_R$ та $R = eP = (x_R, y_R)$.

Введемо функції гешування H_1 та H_2 таким чином:

$$H_1 : \{0,1\}^* \to G,$$

$$H_2 : \{0,1\}^* \to \{0,1\}^{256}.$$

У якості функції $H_1 : \{0,1\}^* \to G$ будемо використовувати функцію Icarta (для поля з характеристикою 2) [3].

Розглянемо докладніше алгоритми, що визначені етапами 5 – 8:

Від повідомлення T обчислюється результат базової функції гешування $H_2(T)$.

Від результату базової функції гешування $H_2(T)$ обчислюється функція Icarta:

Для обраної ЕК виду (1) над скінченним полем F_{2^m}, відображення $x \mapsto x^3$ є бієктивним відображенням. Нехай:

$$H_1 : \{0,1\}^* \to G,$$

$$u \mapsto (x, ux + v^2),$$

де $v = A + u + v^2$ та $x = (v^4 + v^3 + B)^{1/3} + v$.

Функція Icarta відображує елемент скінченого поля у точку на ЕК, що визначається лемою 1.

Лема 1 [3]. Нехай F_{2^m} – поле з непарним m. Для будь-яких $u \in F_{2^m}$, $H_1(u)$ є точкою на кривій

$$E(F_{2^m}) : y^2 + xy = x^3 + Ax^2 + B.$$

Обчислення функції геш-хамелеону виконується за декілька кроків:

Спочатку підписувач випадково обирає ціле число $a \in [1,q]$, та обчислює параметр R:

$$R = (aP, aY).$$

Далі підписувач обчислює параметр S:

$$S = H_1(Y \| I)),$$

де $I = ID_S \| ID_R \| ID_T$ – загальний ідентифікатор, ID_S – ідентифікатор підписувача, ID_R – ідентифікатор одержувача, ID_T – ідентифікатор транзакції [5]. Наступним кроком одержувач обчислює функцію геш-хамелеону H таким чином:

$$H = aP + H_2(T)S,$$

де $H : \{0,1\}^* \to Z_q^*$, T – повідомлення.

Результат обчислення функції геш-хамелеону H_x перетворюється в елемент базового поля h.

Обчислюється передпідпис (e, F_e).

Обчислюється елемент базового поля $t = h + F_e$.

Елемент базового поля t перетворюється на ціле число r.

Обчислюється ціле число $s = (e + dr) \bmod n$.

Значення хамелеон-підпису визначається як $D = (r,s)$.

Обчислення колізії:

одержувач обчислює $R' = (a'P, a'Y)$, де:

$$a'P = aP + (H_2(T) - H_2(T'))S;$$

$$a'Y = aY + z(H_2(T) - H_2(T'))S.$$

Твердження 1. Алгоритм обчислення колізії функції геш-хамелеону є коректним.

Доведення.

$$H' = a'P + H_2(T')S =$$

$$= aP + (H_2(T) - H_2(T'))S + H_2(T')S =$$

$$= aP + H_2(T)S = H \Rightarrow H = H_3(T) = H_3(T')$$

2. Протокол спростування підробленого підпису

Розглянемо протокол спростування підробленого підпису. У подальшому під протиріччям розуміється або відмова підписувача від факту формування ЕЦП, або твердження одержувача про факт підписання хибного повідомлення.

У разі виникнення протиріччя, одержувач надає третій довіреній стороні (ТДС) підпис $D = (T^*, a^*P, a^*Y, r, s)$ та неінтерактивне доведення знання Π_1^* рівності двох дискретних логарифмів $z = \log_P Y = \log_{a^*P} a^*Y$. Якщо D або Π_1^* є недійс-

ними, ТДС відхиляє запит одержувача. Якщо перевірка пройшла успішно, ТДС відправляє підпис підписувачу. Якщо підписувач вважає отриманий підпис дійсним, він підтверджує ТДС цей факт. У протилежному випадку він формує колізію функції гешхамелеону наступним чином:

1. Якщо підписувач хоче забезпечити властивість «відновлення повідомлення», він надає ТДС набір (T, aP, aY, Π_1) у якості колізії, де Π_1 – неінтерактивне доведення знання рівності двох дискретних логарифмів $\log_P aP = \log_Y aY$. Тільки якщо $T^* \neq T$, $H = aP + H_2(T)S$ та Π_1 є дійним, ТДС може бути впевнена у тому, що одержувач сформував підробку підпису повідомлення T. Розгорнутий протокол спростування підробленого підпису у разі необхідності забезпечення властивості «відновлення повідомлення» представлений на рис. 1.

2. Якщо підписувач хоче забезпечити властивість «прихованість повідомлення», він надає ТДС набір (aP, aY, Π_1, Π_2) у якості колізії, де Π_2 – неінтерактивне доведення знання дискретного логарифму $H_2(T) = \log_S(H - aP)$ та Π_1 – неінтерактивне доведення знання рівності двох дискретних логарифмів $\log_P aP = \log_Y aY$.

Тільки якщо, $a^*P \neq aP$, та Π_1, Π_2 є дійсними, ТДС може бути впевнена у тому, що одержувач сформував підробку підпису повідомлення T^*, і водночас, зміст повідомлення T залишається у таємниці.

Розгорнутий протокол спростування підробленого підпису у разі необхідності забезпечення властивості «прихованість повідомлення» представлено на рис. 2.

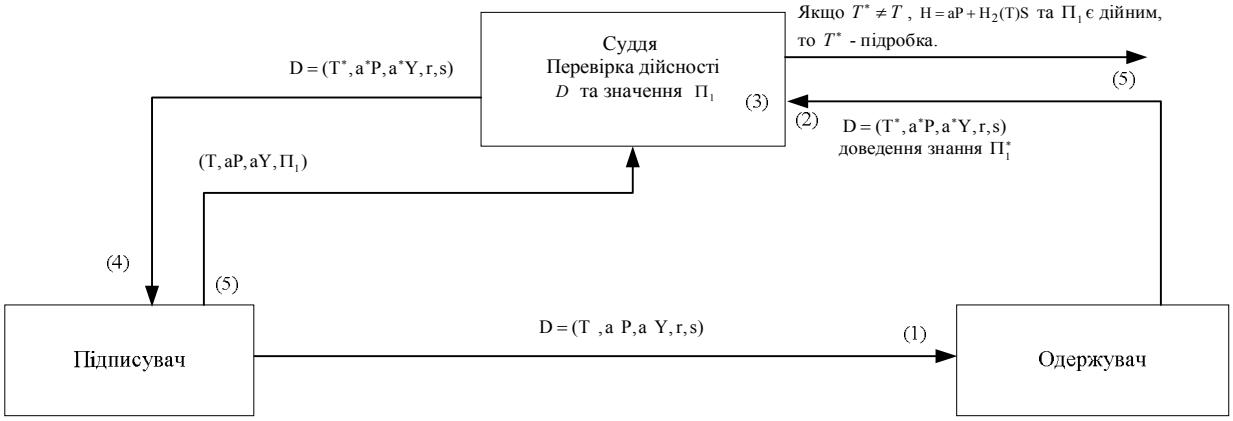

Рис. 1. Розгорнутий протокол спростування підробленого підпису у разі необхідності забезпечення властивості «відновлення повідомлення»

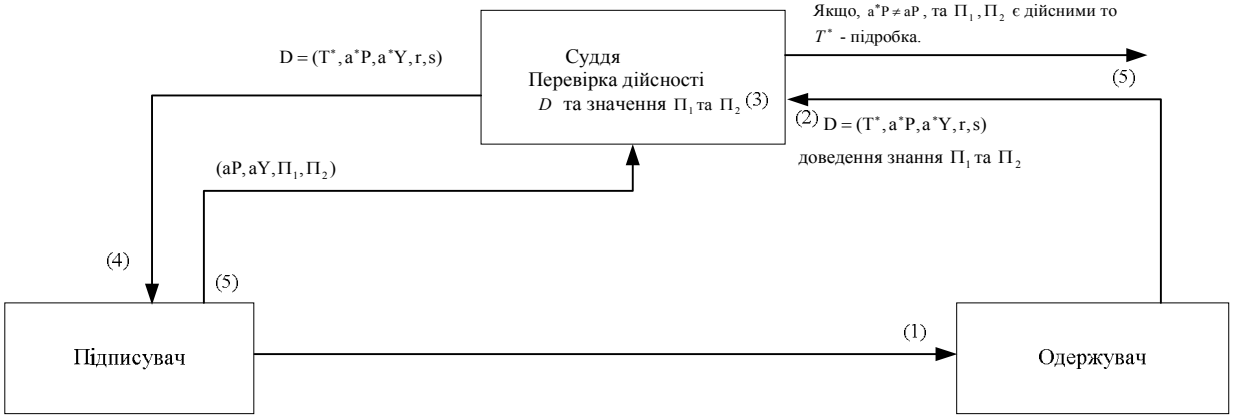

Рис. 2. Розгорнутий протокол спростування підробленого підпису у разі необхідності забезпечення властивості «прихованість повідомлення»

Доведення неінтерактивного знання.

Одержувач хоче довести, що володіє $z \in [2, n-1]$, не розголошуючи його, надаючи підписувачу $\log_P Y$. Підписувач випадковим чином обирає $r \in [2, n-1]$, обчислює $c = H(P, Y, rP)$ та $s = r - cz$, де $H : [0,1]^* \to [0,1]^k$ – колізійно-стійка геш-функція.

Підписувач приймає твердження тоді і тільки тоді, якщо

$$c = H(P, Y, sP + cY).$$

Визначення 1. Пара (c,s), що задовольняє $c = H(P, Y, sP + cY)$ називається доведенням знання значення дискретного логарифму елемента Y за основою P в групі точок ЕК.

Аналогічно визначимо доведення рівності значень двох дискретних логарифмів.

Одержувач обирає $r \in [2, n-1]$ та обчислює:

$$c = H(P_1, P_2, Y_1, Y_2, rP_1, rP_2),$$

$$s = r - cz,\ H : [0,1]^* \to [0,1]^k.$$

Підписувач обчислює:

$$c = H(P_1, P_2, Y_1, Y_2, sP_1 + cY_1, sP_2 + cY_2).$$

Визначення 2. Пара (c,s), що задовольняє $c = H(P_1, P_2, Y_1, Y_2, sP_1 + cY, sP_2 + cY_2)$ називається доведенням рівності знань двох дискретних логарифмів елементів Y_1 та Y_2 за основою P_1 та P_2 в групі точок ЕК.

3 Аналіз стійкості геш-хамелеону в групі точок еліптичної кривої

Для того, щоб геш-функція (поєднання базової геш-функції та функції Icarta) була криптографічно-стійкою вона повинна задовольняти наступним вимогам [6]:

Визначення 3. (Стійкість до знаходження першого прообразу (односторонність)). Геш-функція є стійкою до знаходження першого прообразу, якщо для атакуючого, що має n-бітний рядок (геш-значення) w, обчислювально складно знайти x таке, що $H(x) = w$.

Визначення 4. (Стійкість до знаходження другого прообразу). Геш-функція є стійкою до знаходження другого прообразу, якщо для атакуючого, що має випадковий рядок (повідомлення) x, обчислювально складно знайти $y \neq x$ таке, що $H(x) = H(y)$.

Визначення 5. (Стійкість до колізій). Геш-функція є колізійно-стійкою, якщо для атакуючого, обчислювально складно знайти пару x та y за умови, що $y \neq x$, такі, що $H(x) = H(y)$.

Лема 2 *[6].* Вимога стійкості до знаходження першого прообразу є сильнішою від вимоги стійкості до знаходження другого прообразу та стійкості до колізій.

Лема 3 *[6].* Вимога стійкості до знаходження другого прообразу сильніша від вимоги стійкості до колізій.

Отже, для того, щоб назвати геш-функцію колізійно-стійкою достатньо довести її стійкість до знаходження першого прообразу та стійкість до колізій.

Маючи функцію відображення f у точку на ЕК E, опишемо дві конструкції геш-функцій у E.

Визначимо L як максимальний розмір $f^{-1}(P)$, де P – будь-яка точка на ЕК:

$$L = \max_{P \in E}\left(\left|f^{-1}(P)\right|\right).$$

Для функції $f_{a,b}$ $L \leq 4$, оскільки обернена функція визначається поліномом четвертого степеня. Відмітимо, що якщо ми працюємо у підгрупі E порядку m з кофактором r, ми можемо використовувати функцію $f_{a,b}^{`} = r \times f_{a,b}$. Якщо r є взаємно простим з n, то $L \leq 4r$.

Перша конструкція нашої функції гешування у точку на кривій $E_{a,b}(F_q)$ визначається як:

$$H(m) = f(h(m)),$$

де $h : \{0,1\}^* \mapsto F_q$. Покажемо, що геш-функція H є односторонньою, якщо h – одностороння.

3.1 Односторонність

Визначення 6. Геш-функція є (t,ε) односторонньою, якщо будь-який алгоритм, що виконується за час t, де вхідними даними є $y \in \mathrm{Im}(h)$, на виході буде мати m таке, що $h(m) = y$ з максимальною імовірністю ε. Геш-функція є односторонньою, якщо ε є нехтовно малим для будь-якого поліноміального t.

Зауважимо, якщо використовується одностороння базова геш-функція h, то геш-функція з образом у групі точок ЕК теж буде односторонньою.

Лема 4 [3]. Якщо h є (t,ε)-односторонньою геш-функцією, то H теж є (t',ε')-односторонньою, де $\varepsilon' = L^2\varepsilon$, а $L = \max_{P \in E}\left(\left|f^{-1}(P)\right|\right)$.

Доведення. Подамо на вхід $y = h(m)$ та обчислимо $m' : y = h(m')$, використовуючи алгоритм A, що має за мету зламати односторонність функції H. Маючи $y = h(m)$, ми спочатку обчислимо $f(y) = f(h(m)) = H(m)$ та використаємо A для отримання прообразу $H(m)$. У такому випадку буде виникати дві проблеми:

1. $f(y)$ не буде мати рівномірного розподілу, навіть якщо y – рівномірно розподілена.

2. Прообраз m' для $H(m)$ не обов'язково буде прообразом y.

Нехай A – алгоритм, що обчислює прообраз за час t з ймовірністю не менше ніж ε'. Нехай S буде випадком, у якому A – реалізований успішно. Коли A отримує на вхід P, що має рівномірний розподіл у $\mathrm{Im}(H)$, маємо:

$$\Pr[S] = \sum_{p \in Im(H)} \Pr[S|P = p] \frac{1}{|Im(H)|} \geq \varepsilon' .$$

Однак, у якості вхідних даних для A, ми використовуємо $f(y)$, що не має рівномірного розподілу, навіть якщо y – має.

Таким чином, необхідно обчислити ймовірність успіху A, маючи P обчислену як $f(y)$. Нехай $\Pr(S')$ визначає ймовірність успіху. Отримаємо:

$$\Pr[S'] = \sum_{p \in Im(H)} \Pr[S|P = p] \frac{1}{|Im(H)|} \geq$$

$$\geq \sum_{p \in Im(H)} \Pr[S|P = p] \frac{1}{L|Im(H)|} \geq \frac{\varepsilon'}{L} .$$

Це доводить, що A має ймовірність успіху обчислення прообразу $f(y) = H(m)$ не менше ε'/L.

Припустимо, що A успішно обчислив один прообраз $f(y)$. Так як кожна точка має L прообразів функції f, цей прообраз є прообразом $y = h(m)$ з ймовірністю $1/L$. Мається на увазі, що алгоритм має ймовірність успіху не менше ε'/L^2, а $\varepsilon'/L^2 \leq \varepsilon$.

3.2 Стійкість до колізій

Визначення 7 [3]. Сімейство геш-функцій H є (t, ε) колізійно-стійким, якщо будь-який алгоритм, що виконується за час t, маючи у якості вхідних даних випадкову функцію $h \in H$, знайде $m, m' : h(m) = h(m')$ з ймовірністю не більше ніж ε.

Перша конструкція може бути легко розширена для сімейства геш-функцій: маючи сімейство геш-функцій H, визначимо для кожної $h \in H$ функцію $H = f \circ h$.

Колізія функції H існує тоді і тільки тоді:

1. Коли існують $m, m' : h(m) = h(m')$, це колізія h,
2. Коли $f(u) = f(u')$ для $u = h(m)$, $u' = h(m')$ за умови, що $u \neq u'$, це колізія f.

Відмітимо, що ми не можемо довести стійкість до колізій H, базуючись лише на стійкості до колізій h. Тобто, маючи геш-функцію h, легко побудувати ЕК з колізією на $H = f_{a,b} \circ h$. Нехай, для (m, m'), $u = h(m)$ та $u' = h(m')$. Для пари (u, u'), обчислимо поліном 4-го ступеня:

$$(X - u)(X - u')(X^2 + (u + u')X - w),$$

де w випадково обраний елемент з F_q. Цей поліном є еквівалентним до:

$$X^4 - 6xX^2 + 6yX - 3a,$$

де $$x = -\frac{uu' + w - (u + u')^2}{6};$$

$$y = \frac{(u + u')(uu' - w)}{6}, \quad a = -\frac{uu'w}{3}.$$

Нехай $b = y^2 - x^3 - ax$. Так як (x, y) – точка на ЕК $E_{a,b}$, то прообраз (x, y) є розв'язком рівняння:

$$X^4 - 6xX^2 + 6yX - 3a = 0,$$

Тому, u та u' є розв'язками вищенаведеного рівняння та прообразами (x, y). Отже, (m, m') є колізією для $H = f_{a,b} \circ h$. Однак, якщо $E_{a,b}$ визначено незалежно від h, здається складно обчислити $(m, m') : f_{a,b}(y) = f_{a,b}(y')$, де $y = h(m)$ та $y' = h(m')$. У цьому випадку, H має бути колізійно-стійкою. Ми не можемо довести, що H – колізійно-стійка, базуючись лише на колізійній стійкості h. Отже необхідні деякі додаткові властивості функції h. Далі ми розглянемо конструкцію, для якої стійкість до колізій доводиться за рахунок стійкості h.

Тобто, у випадку, коли зловмисник має можливість обирати параметри ЕК незалежно від вибору базової функції гешування h, функція Icarta не буде колізійно-стійкою. Але у відомих криптопротоколах, що базуються на криптоперетвореннях в групі точок ЕК, у яких може бути застосований геш-хамелеон в групі точок ЕК, параметри ЕК обираються на етапі вибору загальносистемних параметрів, а отже до вибору базової функції гешування і незалежно від неї. А це означає, що атака, яка заснована на довільному виборі параметрів ЕК не може бути реалізована. Отже, зважаючи на застосування запропонованого геш-хамелеону у існуючих криптопротоколах ЕЦП, можна стверджувати, що поєднання базової функції гешування та функції Icarta є колізійно-стійкою конструкцією.

Твердження 2. Запропонований протокол геш-хамелеону в групі точок ЕК є колізійно-стійким, спираючись на твердження, що обчислювальна задача Діффі-Гелмана у групі точок ЕК $E(F_{2^m})$ є важкорозв'язною.

Доведення від протилежного. Нехай існує алгоритм A, що дозволить знайти розв'язок за поліноміальний час, який представить дві пари (T, R) та (T', R'), що задовольнять рівняння:

$$a'P + H_2(T')S = aP + H_2(T)S .$$

Це означало б, що ми маємо змогу ефективно вирішити рівняння:

$$zS = (a'Y / aY)^{(H_2(T) - H_2(T'))^{-1}},$$

а це еквівалентно вирішенню обчислювальної задачі Діффі-Гелмана у групі точок ЕК $E(F_{2^m})$.

Висновки

Розроблений протокол хамелеон-підпису дозволяє розширити сферу застосування національного стандарту ДСТУ 4145-2002 за рахунок впровадження геш-хамелеону.

Вдосконалений протокол ДСТУ 4145-2002 володіє властивостями, які дозволяють забезпечувати прихованість повідомлення та непередаваність сформованого ЕЦП.

Зазначені властивості дозволяють застосовувати вдосконалений протокол ДСТУ 4145-2002, як функцію криптографічної підтримки послуг захисту від несанкціонованого доступу у частині забезпечення послуги анонімності.

Новизна отриманих результатів полягає у:

1) розробці геш-хамелеону у групі точок ЕК, що використовує такі ж системні параметри, що і базовий алгоритм ЕЦП ДСТУ 4145-2002;

2) обґрунтуванні вимог та виборі функції гешування у точку на ЕК;

3) отриманні теоретичних оцінок стійкості вдосконаленого протоколу ДСТУ 4145-2002.

Література

1. ISO/IEC 15408. Information technology – Security techniques – Evaluation criteria for IT security.

2. ДСТУ 4145-2002 "Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння". – К.: Держспоживстандарт України, 2002. – 44 с.

3. Icart, T. How to hash into elliptic curves [Text] / T. Icart // Proc. of Crypto 2009. – Springer, 2009. – Vol. 5677. – P 303 – 316.

4. Krawczyk, H. Chameleon hashing and signatures [Text] / H. Krawczyk, T. Rabin // Proc. of NDSS. – 2000. – P. 143 – 154.

5. Chen, X. Key-Exposure Free Chameleon Hashing and Signatures Based on Discrete Logarithm Systems [Text] / X. Chen, F. Zhang. – Cryptology ePrint Archive: Report 2009/035, 2009. – 80 p.

6. Mironov, I. Hash functions: Theory, attacks, and applications [Text] / I. Mironov. – Technical Report, MSR-TR-2005-187, Microsoft Research, November 2005. – 230 p.

Надійшла до редакції 22.07.2011

Рецензент: д-р техн. наук, проф. начальник кафедри О.В. Потій, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

ПРОТОКОЛ ХАМЕЛЕОН-ПОДПИСИ НА ОСНОВЕ СТАНДАРТА ДСТУ 4145-2002 С ИСПОЛЬЗОВАНИЕМ ХЕШ-ХАМЕЛЕОНА В ГРУППЕ ТОЧЕК ЭЛЛИПТИЧЕСКОЙ КРИВОЙ

К.А. Погребняк, Ю.М. Леншина

Предлагается протокол хамелеон-подписи на основе национального стандарта ДСТУ 4145-2002 с использованием хеш-хамелеона в группе точек эллиптической кривой, обеспечивающий свойства непередаваемости подписи и скрытости сообщения. Обосновывается выбор функции хеширования в точку на эллиптической кривой, необходимой для хамелеон-подписи на основе стандарта ДСТУ 4145-2002. Приводятся расширенные протоколы опровержения подделанной подписи для случаев обеспечения свойства скрытости сообщения и свойства восстановления сообщения. Приводится доказательство стойкости предложенного протокола хеш-хамелеона и хамелеон-подписи.

Ключевые слова: хеш-хамелеон, хамелеон-подпись, группа точек ЭК, функция отображения, электронная цифровая подпись.

THE PROTOCOL OF CHAMELEON-SIGNATURE BASED ON THE STANDARD DSTU 4145-2002 USING CHAMELEON-HASH IN THE GROUP OF POINTS ON AN ELLIPTIC CURVE

K.A. Pogrebnyak, Ju.M. Lyenshyna

The protocol of chameleon-signature based on the national standard DSTU 4145-2002 using chameleon-hash in the group of points on an elliptic curve has the properties of non-transferability and message hiding is proposed. The choice of the hash function to a point on an elliptic curve required for the chameleon-signature based on the standard DSTU 4145-2002 is substantiated. Extended protocols of denial signatures for the cases to ensure properties of non-transferability and message hiding are provided. The resistance proof of the proposed chameleon hash protocol and chameleon signatures are provided.

Keywords: chameleon-hash, chameleon signature, the group of points on an EC, map function, digital signature.

Погребняк Костянтин Анатолійович – канд. техн. наук, начальник відділу криптографічного захисту інформації, ПАТ "Інститут інформаційних технологій ", Харків, Україна, e-mail: iitkostya@gmail.com.

Лєншина Юлія Михайлівна – фахівець з систем захисту інформації, ПАТ "Інститут інформаційних технологій ", Харків, Україна, e-mail: ki_sk@rambler.ru.