УДК 681.3.06

К.А. Погребняк, Ю.М. Лєншина

Приватне акціонерне товариство «Інститут інформаційних технологій», Харків

ГЕШ-ХАМЕЛЕОН В ГРУПІ ТОЧОК ЕЛІПТИЧНОЇ КРИВОЇ

Пропонується алгоритм обчислення функції геш-хамелеону в групі точок еліптичної кривої з метою впровадження у національний стандарт електронного цифрового підпису ДСТУ 4145-2002. Обґрунтовується вибір функції гешування у точку на еліптичний кривій, що необхідна для хамелеон-підпису на основі стандарту ДСТУ 4145-2002.

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

Вступ

Електронні системи комерції, без яких сьогодні неможливе якісне управління інформатизованими бізнес-процесами в Україні, потребують їх удосконалення у зв'язку з необхідністю забезпечення послуги анонімності дій користувачів разом з послугами неспростовності джерела та цілісності інформації. Протоколом забезпечення послуг неспростовності джерела та цілісності інформації в Україні, яких раніше було достатньо, є протокол електронного цифрового підпису (ЕЦП) згідно стандарту ДСТУ 4145 -2002 [1]. Національною системою ЕЦП є Інфраструктура відкритих ключів (ІВК), але вона не надає можливості забезпечення анонімності дій користувачів, адже стандарт ДСТУ 4145-2002 накладає певні функціональні обмеження. У статті пропонується створення функції геш-хамелеону в групі точок еліптичної кривої. Впровадження створеного геш-хамелеону у ДСТУ 4145-2002 дозволить забезпечити послугу анонімності дій користувачів, без створення обмежень для забезпечення послуг неспростовності джерела та цілісності інформації.

Слід відмітити, що для функції геш-хамелеону в групі точок еліптичної кривої необхідна функція відображення в точку на еліптичній кривій (з заданими у ДСТУ 4145-2002 параметрами). З метою вирішення цієї задачі проводиться аналіз існуючих функцій відображення в точку на ЕК та обґрунтовується вибір функцій з необхідними параметрами. Отже, у статті пропонується удосконалена функція геш-хамелеону в групі точок еліптичної кривої, з метою її впровадження у національний стандарт ЕЦП ДСТУ 4145-2002.

1. Алгоритм обчислення геш-хамелеону в групі точок еліптичної кривої

Алгоритм обчислення геш-хамелеону в групі точок еліптичної кривої (структурна схема представлена на рис.1) складається з таких етапів:

– обчислення загальних параметрів геш-хамелеону;

– обчислення секретного та відкритого ключів геш-хамелеону;

– обчислення функції геш-хамелеону.

На етапі Обчислення загальних параметрів геш-хамелеону обирається група точок еліптичної кривої виду:

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

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

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. Введемо функції гешування H_1 та H_2 таким чином:

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

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

Відмітимо, що функція H_2 визначається стандартом ГОСТ 34.311-95.

Загальносистемними параметрами геш-хамелеону будуть:

$$\left\{F_{2^m}, E, P, q, H_1, H_2\right\}.$$

На етапі Обчислення секретного та відкритого ключів геш-хамелеону спочатку одержувач випадковим чином обирає секретний ключ $x \in [1,q]$, і потім обчислює відкритий ключ як $Y = xP$.

Обчислення функції геш-хамелеону виконується за декілька кроків.

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

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

Далі одержувач 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. Останнім кроком одержувач обчислює функцію геш-хамелеону $H = H_3(T) = H_x$ наступним чином:

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

де $H_3 : \{0,1\}^* \to Z_q^*$, T – повідомлення, H_x – абсциса точки H.

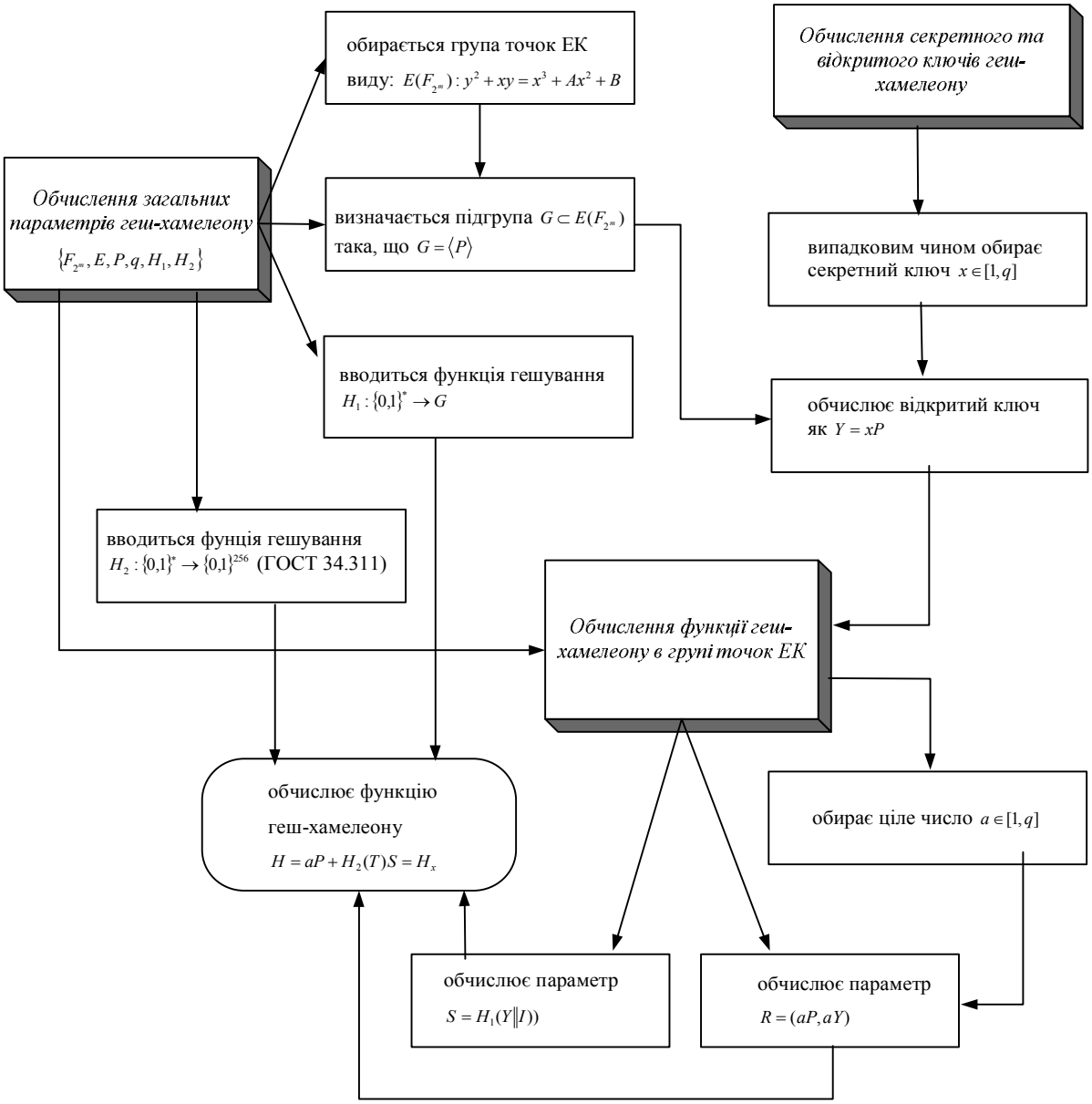

Рис. 1. Структурна схема геш-хамелеону в групі точок ЕК

Обчислення колізії:

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

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

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

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

Доведення.

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

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

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

Твердження 2. Запропонована схема є колізійно-стійкою, 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:

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

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

2. Вибір функції гешування у точку на ЕК

Як було зазначено раніше, схема геш-хамелеону в групі точок еліптичної кривої створювалася з метою удосконалення діючого в Україні стандарту ЕЦП ДСТУ 4145-2002 [1]. Отже нам необхідно обрати функцію гешування у точку на еліп-

тичній кривій, параметри якої не суперечили б визначеним у стандарті (з метою максимального узгодження загальносистемних параметрів геш-хамелеону та базового протоколу ЕЦП згідно ДСТУ 4145-2002). Розглянемо докладніше функції, що відповідають нашим вимогам, а отже можуть бути застосовані у запропонованій схемі геш-хамелеону в групі точок ЕК, у якості функції $H_1 : \{0,1\}^* \to G$.

Багато криптосистем на еліптичних кривих потребують наявності функції хешування із образом в групі точок еліптичної кривої. Першим приклад такої геш-функції, було представлено у роботі Boneh та Franklin [2]. Вони використовували специфічний вид кривої – суперсингулярну криву, що забезпечувала взаємно-однозначне відображення f з мультиплікативної групи базового поля F_p у адитивну групу точок еліптичної кривої $E(F_p)$, та визначили цю геш-функцію, як:

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

де h – класична геш-функція, що відображає елемент з $\{0,1\}^*$ в елемент базового поля F_p. Boneh та Franklin довели, що їх IBE (identity-based encryption) схема є захищеною, коли геш-функція h поводить себе, як випадковий оракул у F_p (тобто, їм не потрібно припускати, що H є випадковим оракулом у $E(F_p)$).

Але така конструкція геш-функції не має сенсу у загальному випадку, оскільки умови її застосування полягають у використанні суперсингулярних кривих. Такий клас еліптичних кривих на поточний момент застосовується виключно у криптографічних додатках, що базуються на використанні ідентифікаторів (identity-based cryptography).

Національна система ЕЦП визначається стандартом ДСТУ 4145-2002, що використовує еліптичні криві над розширеними полями характеристики два. Одна з умов, яку повинні задовольняти еліптичні криві практичного застосування, – це MOV-умова. Слід зазначити, що всі суперсингулярні криві не задовольняють зазначеній умові.

Відомими підходами по побудуванню геш-функцій з образом у групі точок загальної еліптичної кривої є імовірнісний та детермінований.

Імовірнісний підхід гешування у точку на ЕК

Класичним підходом з 2004 року є імовірнісний підхід відображення у точку на еліптичній кривій, що отримав назву Try and Increment [3].

Алгоритм Try and Increment виконується таким чином:

Вхідні дані алгоритму: ціле число u, еліптична крива $E(F_{p^n})$, де $p > 3$, вигляду $Y^2 = X^3 + aX + b$, де $a, b \in F_{p^n}$.

Вихідні дані: Q – точка на кривій $E_{a,b}(F_q)$.

1. For $i = 0$ до $k - 1$:
   - обчислюється $x = u + i$;
   - if $x^3 + ax + b$ є квадратичним лишком у F_q, то $Q = (x, (x^3 + ax + b)^{1/2})$.
2. End for.
3. Return.

Однак цей підхід потребує значних часових витрат, що є не бажаним у багатьох інформаційних системах. Очевидно також, що у випадку застосування імовірнісного підходу, дуже важко точно оцінити захищеність криптосистеми. Отже важливою задачею є знаходження алгоритму гешування в точку на еліптичній кривій, який виконувався б за детермінований проміжок часу та піддавався б більш точному аналізу.

Детерміновані підходи гешування у точку на ЕК.

Першим алгоритмом гешування у точку на ЕК за детермінований час був, представлений у роботі Shallue [4], і пізніше спрощений та розширений для випадку застосування гіпереліптичних кривих Ulas [5]. Потім Icart у роботах [6, 7] відновив інтерес до таких алгоритмів гешування, як для випадку застосування звичайних ЕК, так і для гіпереліптичних кривих. Детерміновані підходи гешування у точку на ЕК та ГЕК можна умовно поділити на два види:

SWU-подібне гешування, запропоноване Shallue-Woestijne-Ulas [4, 5, 8], що базується на побудуванні раціональних кривих на поверхні, які асоційовані з базовою еліптичною кривою.

Icart-побідне гешування, що запропоноване Icart [6 – 8], полягає у явному поданні формул знаходження нулів еліптичної кривої.

Проаналізувавши дані, що представлені у табл. 1, ми бачимо можливість застосування двох функцій, параметри яких не суперечать визначеним у стандарті [1]. (характеристика базового поля 2), а саме SWU-подібній геш-функції, визначеній у [5] та Icart-подібній геш-функції, визначеній у [7].

3. Геш-функції Shallue-Woestijne та Icarta

3.1. Гешування Shallue-Woestijne у точку на ЕК. У 2006 році Shallue та Woestijne у роботі [4] представили новий алгоритм гешування у точку на ЕК за детермінований поліноміальний час, що базується на рівності Skalba [9].

Нехай ЕК визначається рівнянням:

$$f(x) = x^3 + ax + b.$$

Існує чотири відображення $X_1(t), X_2(t), X_3(t), X_4(t)$ такі, що:

$$f(X_1(t)) \times f(X_2(t)) \times f(X_3(t)) \times f(X_4(t)) = X_4(t)^2.$$

Таблиця 1

Результати аналізу підходів детермінованого гешування у точку на ЕК

	Характерристика поля	Рівняння кривої	Джерело аналізу	Умова
SWU-подібні	$\neq 2,3$	$y^2 = x^3 + ax + b$	SW[4]	–
			Simp. SWU[5]	$q \equiv 3 (\mathrm{mod}\, 4)$
	2	$y^2 + xy = x^3 + ax^2 + b$	**SW[4]**	–
Icart-подібні	$\neq 2,3$	$y^2 = x^3 + ax + b$	Icart [10]	$q \equiv 2 (\mathrm{mod}\, 3)$
	2	$y^2 + xy = x^3 + ax^2 + b$	**Icart [7]**	$q \equiv 2 (\mathrm{mod}\, 3)$

У скінченному полі, для фіксованого параметру t, хоча б один з $f(X_i(t))$ повинен бути квадратичним лишком, це означає, що ця $f(X_i(t))$ є абсцисою точки на ЕК $y^2 = f(x)$.

Для того, щоб обчислити вираз $f(X_1(t)) \times f(X_2(t)) \times f(X_3(t)) \times f(X_4(t)) = X_4(t)^2$ та обрати серед $f(X_i(t))$ необхідно обчислити квадратний корінь у F_q. Обчислення квадратних коренів у F_q може бути виконано за імовірнісний поліноміальний час, із застосуванням алгоритму Tonelli-Shanks. Завдяки рівності Skalba, автори роботи [9], показали як робити це за детермінований час, використовуючи модифікацію алгоритма Tonelli-Shanks, за час $O(\log^4 q)$. Занотуємо, що для $q = 3 \bmod 4$, обчислення квадратного кореня виконується за $O(\log^3 q)$. Завдяки цьому, алгоритм Shallue-Woestijne виконується за час $O(\log^4 q)$ для будь якого розміру поля $q = p^n$, та за час $O(\log^3 q)$ при дотриманні умови $q = 3 \bmod 4$.

3.2. Функція Icarta для випадку характеристики поля p. Нехай ЕК визначається рівнянням

$$E_{a,b} : Y^2 = X^3 + aX + b \text{ над полем } F_{p^n},$$

де $p > 3$ та $p^n = 2 \bmod 3$ [7, 10].

У таких скінченних полях, функція $x \mapsto x^3$ є бієктивним відображенням з інверсною функцією:

$$x \mapsto x^{1/3} = x^{(2p^n - 1)/3}.$$

Це дозволяє створити параметризацію підмножини ЕК $E_{a,b}(F_{p^n})$. Нехай:

$$f_{a,b} : F_{p^n} \mapsto E_{a,b}; \qquad u \mapsto (x, y),$$

де $x = (v^2 - b - \frac{u^6}{27})^{1/3} + \frac{u^2}{3}$, $y = ux + v$, $v = \frac{3a - u^4}{6u}$.

Для $u = 0$, де $f_{a,b}(0) = O$ – нейтральний елемент ЕК.

3.3 Функція Icarta для випадку характеристики поля 2. Позначимо скінченне поле як F_q, де $q = 2^m$. Визначимо вид еліптичної кривої:

$$y^2 + xy = x^3 + ax^2 + b,$$

де $a, b \in F_{2^m}$, $b \neq 0$. Для випадку, коли m – непарне, відображення $x \mapsto x^3$ є бієктивним відображенням. Нехай:

$$f_{a,b} : F_{2^n} \to E(F_{2^n}); \qquad u \mapsto (x, ux + v^2),$$

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

Таким чином, Функція Icarta для випадку характеристики поля 2 задовольняє вимогам застосування геш-хамелеону на основі ЕК разом зі схемою ЕЦП згідно стандарту ДСТУ 4145-2002 в умовах використання однакових загальносистемних параметрів. Розглянемо властивості обраної геш-функції.

Властивості геш-функції Icarta.

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 n з кофактором r, ми можемо використовувати функцію $f'_{a,b} = r \times f_{a,b}$. Якщо r є взаємно простим з n, то $L \leq 4r$.

Функція 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.

Визначення. 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 одностороння.

Лема [7]. Якщо h є (t, ε)-односторонньою геш-функцією, то H теж є (t, ε)-односторонньою, де $\varepsilon' = L^2 \varepsilon$.

Таким чином, при використанні ГОСТ 34.311 у якості базової функції гешування для геш-функції Icarta отримаємо загальну геш-функцію із образом у групі точок ЕК, що є односторонньою.

Висновки

Вимоги до сучасних систем електронної комерції потребують забезпечення анонімності дій користувачів. Ця властивість забезпечується функцією геш-хамелеону, що разом з ЕЦП має назву хамелеон-підпис.

Впровадження відомих (таких, що базуються на складності вирішення задачі факторизації або дискретного логарифму [11 – 13]) функцій геш-хамелеону, у національний стандарт ДСТУ 4145-2002 призводить до виникнення проблем пов'язаних із зростанням кількості загальносистемних параметрів результуючої схеми та ускладненням задачі забезпечення їх узгодженості.

У роботі запропоновано нову функцію геш-хамелеону, стійкість якої базується на складності вирішення задачі дискретного логарифму у групі точок ЕК та використовує загальносистемні параметри, що визначені для схеми ЕЦП за ДСТУ 4145-2002.

Впровадження запропонованого геш-хамелеону до схеми ЕЦП за ДСТУ 4145-2002 потребує розв'язання задачі гешування у точку на ЕК. У ході проведеного порівняльного аналізу існуючих (імовірнісних та детермінованих) підходів до гешування у точку на ЕК за критеріями: стійкості, складності та узгодженості із параметрами визначеними у ДСТУ 4145-2002, у якості перетворення, що дозволяє виконувати гешування у точку на ЕК, було обґрунтовано використання функції Icarta.

Сукупність отриманих результатів можна вважати теоретичною основою для створення функції хамелеон-підпису на основі схеми ЕЦП за ДСТУ 4145-2002, що дозволяє без зниження стійкості забезпечити нові властивості (непередаваності підпису та прихованості повідомлення) у діючий інфраструктурі відкритих ключів.

Список літератури

1. ДСТУ 4145-2002 "Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння".

2. Boneh D. Franklin. Identity-based encryption from the weil pairing / D. Boneh, K. Matthew // In Joe Kilian, editor, CRYPTO. – Springer, 2001. – Volume 2139 of Lecture Notes in Computer Science. – P. 213-229.

3. Boneh D. Short signatures from the weil pairing / D. Boneh, B. Lynn, and H. Shacham // J. Cryptology. – 2004. – 17 (4). – P. 297-319.

4. Shallue A. Construction of rational points on elliptic curves over finite fields / A. Shallue, C. van de Woestijne // ANTS. – Springer, 2006. – Vol. 4076 of Lecture Notes in Computer Science. – P. 510-524 .

5. Ulas M. Rational points on certain hyperelliptic curves over finite fields / M. Ulas // Bull. Polish Acad. Sci. Math. – 2007. – 55(2). – P. 97-104.

6. Efficient indifferentiable hashing to elliptic curves / E. Brier, J.-S. Coron, T. Icart, D. Madore, H. Randriam, M. Tibouchi // Proceedings of CRYPTO 2010, lncs, Springer-Verlag, 2010.

7. T. Icart, How to hash into elliptic curves, Proceedings of Crypto 2009, lncs, vol. 5677, pp. 303-316, Springer, 2009.

8. Farashahi R.R. On hashing into elliptic curves / R.R. Farashahi, I. Shparlinski, J.F. Voloch // J.Math. Crypt. – 2009. – Vol. 3 (10). – P. 353-360.

9. Skalba M. Points on elliptic curves over finite fields / M. Skalba // Acta Arith. – 2005. – 117 (3). – P. 293-301.

10. Fouque P.-A. Estimating the size of the image of deterministic hash functions to elliptic curves / P.-A. Fouque, M. Tibouchi // In M. Abdalla and P. Baretto, editors, LATINCRYPT, Lecture Notes in Computer Science. – Springer, 2010.

11. Krawczyk H. Chameleon hashing and signatures / H. Krawczyk, T. Rabin // Proc. of NDSS 2000. – P. 143-154.

12. Лєншин А.В. Додаткові властивості безпеки електронних транзакцій у системах, що використовують сервіси комбінованої ІВК / А.В. Лєншин, Ю.М. Іщенко // Вісник ХНУ ім. В.Н. Каразіна №890. Серія "Математичне моделювання. Інформаційні технології. Автоматизовані системи управління". – Х., 2010. – Вип. 13. – С. 109-114.

13. Лєншина Ю.М. Реалізація послуги приватності у схемі інтернет-аукціону з використанням хамелеон-підпису / Ю.М. Лєншина, Д.С. Беляк,// Системи обробки інформації. – Х., 2011. – Вип. 3 (93). – С. 126-129.

Надійшла до редколегії 22.08.2011

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

ХЕШ-ХАМЕЛЕОН В ГРУППЕ ТОЧЕК ЭЛЛИПТИЧЕСКОЙ КРИВОЙ

К.А. Погребняк, Ю.М. Леншина

Предлагается алгоритм вычисления функции хеш-хамелеона в группе точек эллиптической кривой с целью его внедрения в национальный стандарт электронной цифровой подписи ДСТУ 4145-2002. Обосновывается выбор функции хеширования в точку на эллиптической кривой, которая необходима для хамелеон-подписи на основе стандарта ДСТУ 4145-2002.

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

CHAMELEON HASH IN THE GROUP OF POINTS ON THE ELLIPTIC CURVE

K.A. Pogrebnyak, I.M. Lyenshyna

The algorithm for computing the function of chameleon-hash in the group of points on the elliptic curve with a view to its deployment into the national standard of digital signature DSTU 4145-2002 is proposed. The choice of chameleon-hash function to a point on the elliptic curve, which is necessary for the chameleon-signature based on the standard DSTU 4145-2002 is substantiated.

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